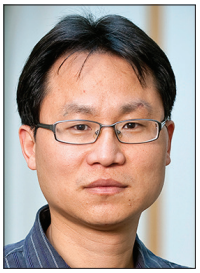
Vehicular Networking Series Editorial

Protecting Vehicles from Imminent Cyber Threats

Anwer Al-Dulaimi



Xiaodong Lin

Vehicular networking continues to evolve, along with other segments of wireless networks, toward efficient networks that connect everything, anytime, anywhere. With this understanding, the arrival of the fifth generation (5G) technologies will provide the underlying infrastructure and radio access interfaces to support highly efficient communications for connected vehicles. While researchers remain focused on developing location identification for autonomous cars, most research activities bypass the security concerns for this type of critical communications, which are directly associated with human safety. There are two main segments for vehicular networking: first, the platforms that support data collection and communications; and second, the operational software and data resources. Considering platforms, the various sensors in the vehicle are the basic front-end data collectors that help monitoring systems to identify key performance indicators about physical platform status. The communication system that is mounted on a vehicle is the component that packetizes data and exchanges them with the surrounding mobile and fixed transmitters. The software layer involves the over-the-top operational processes and services that define platform functionalities and control them. Although autonomous cars have access to data resources through wireless communication to operate efficiently and safely without human intervention, they are still vulnerable to cyber-attacks like any other computational systems. Therefore, we need to look at vehicular communications from end to end rather than as segregated systems.

The communications between autonomous cars and the environment can be classified into two categories: communications to other cars and communications with the network. Considering communications with surrounding cars, the blockchain emerges as the scheme with the highest potential to manage data sharing between participating vehicles. However, the validation of participants and shared data remain major challenges for such a model, which threatens the safety of any vehicle acquiring invalid data from this scheme. Therefore, there might be a need to develop new blockchain models that adhere to vehicular networking requirements of defining the proper data initiators before accepting their involvement in any chain. Considering network infrastructure, autonomous cars are just other subscribers to the communication system that can be targeted by cyber-attacks and malicious threats. It is important to keep in mind that operators do not themselves face such imminent threats and cannot be held accountable when it comes to vehicles' safety. The challenge of securing communications and optimizing connectivity with vehicles escalates considering the wide deployment of clouds within operators' infrastructure.

This issue has two articles. The first article, "Vehicular Communications: Standardization and Open Issues" by Liang Zhao *et al.*, studies the current standardization, frequency, and testing of dedicated short-range communications (DSRC) and Long Term Evolution vehicle-to-everything (LTE-V2X), respectively. The article reviews the state of the art of DSRC and LTE-V2X with a comprehensive comparison between those technologies considering different parameters along with potential evolution aspects. The authors propose a software defined vehicular network (SDVN) architecture that combines multiple communication technologies to support fully autonomous driving solutions for future vehicular communications using DSRC and LTE-V2X technologies.

The second article, "RepGuide: Reputation-Based Route Guidance Using Internet of Vehicles Vehicular Networking" by Muhammad Awais Javed and Sherali Zeadally, studies the challenge of malicious vehicles that transmit wrong traffic information, deliberately feeding no accurate data to route decision units. The article starts by reviewing the wireless traffic information exchange between vehicles and infrastructure roadside units (RSUs) to form a ubiquitous connected network known as the Internet of (connected) Vehicles (IoV), and also surveys related standardization recommendations by vehicular environment (WAVE) and European Telecommunications Standards Institute (ETSI) Intelligent Transport Systems (ITS). Finally, the authors propose an algorithm that verifies the suspicious traffic information by multihop communication exchange with vehicles outside the transmission range of the RSU.

Biographies

Anwer Al-Dulaimi [M'11, SM'17] (anwer.al-dulaimi@exfo.com) received his Ph.D. degree in electrical and electronic engineering from Brunel University, London, United Kingdom, in 2012. Currently, he is a system engineering specialist in the R&D Department at EXFO, Toronto, Canada. His research interests include 5G, dynamic spectrum access, cloud networks, and V2X. He is the chair of the IEEE 1932.1 Working Group "Standard for Licensed/Unlicensed Spectrum Interoperability in Wireless Mobile Network" and Editor of the IEEE 5G Initiative Series.

Xiaodong Lin [GS'06, M'08, SM'12, F'17] (xlin@wlu.ca) received his Ph.D. degree (with the Outstanding Achievement in Graduate Studies Award) in electrical and computer engineering from the University of Waterloo, Canada, in 2008. He is currently an associate professor of computer science with the Department of Physics & Computer Science at Wilfrid Laurier University, Canada. His research interests include wireless network security, applied cryptography, computer forensics, software security, and wireless networking and mobile computing.