SECURE WIRELESS COMMUNICATIONS FOR VEHICLE-TO-EVERYTHING

Vuk Marojevic

Charles Kamhoua

Jeffrey Reed

Friedrich Jondral

Intelligent transportation systems (ITS) will support more efficient vehicular traffic flow, increased vehicular and pedestrian safety, and, eventually, autonomous driving. Wireless communications is fundamental for enabling ITS, and recent advances in communications technology and systems support establishing reliable wireless links and networks among cars, cars and pedestrians, and cars and fixed infrastructure. The success of ITS will be measured in terms of how well it can scale to the ever-increasing mobility application scenarios and harsh environmental conditions. Research and development is ongoing to make vehicle-to-everything (V2X) systems more reliable and more secure for providing safety-critical applications. This Feature Topic brings together researchers and practitioners in V2X security to share their latest research contributions and expert insights.

The first article, "MBID: Micro-Blockchain Based Geographical Dynamic Intrusion Detection for V2X" by Haoran Liang *et al.*, outlines an original scheme for geographical dynamic intrusion detection in V2X settings using a multi-tiered blockchain architecture. The architecture allows the micro-blockchains to be repeatedly nested to deliver tamper-resistant intrusion detection strategies. The topic is timely, and the fragmentation of blockchains into multiple smaller parts is gaining increasing attention in various fields.

The second article, "Physical-Layer Security and Privacy for Vehicle-to-Everything" by Basem M. ElHalawany *et al.*, provides an overview on physical-layer security strategies against eavesdropping employed in vehicular networks. It summarizes ongoing research topics in this area and points to open issues and future research challenges with applications to different V2X network architectures and communication standards. Simulation results for a practical case study highlight the benefits of exploiting moving relays and non-orthogonal multiple access for physical-layer security in V2X.

The next article is "Unmanned Aerial Vehicle (UAV) Meets Vehicle-to-Everything in Secure Communications," written by Bodong Shang *et al.* It proposes UAV-assisted security enhancements of terrestrial wireless communications systems, such as cellular networks, and introduces several UAV use cases that leverage advanced wireless technology to improve the communications security of vehicular users. The authors show clear advantages of using aerial over terrestrial jammers for improving the secrecy rate against eavesdropping and highlight research and development problems that require an interdisciplinary approach.

The final article, "Predictive Cruise Control with Private Vehicle-to-Vehicle Communication for Improving Fuel Consumption and Emissions" by Xueru Zhang *et al.*, describes a privacy-preserving approach for the exchange of vehicle speed information in predictive cruise control applications. Such predictive controllers can be sensitive to perturbations added to the communicated signals for improved privacy. The proposed approach achieves sufficient accuracy for predictive control purposes while preserving privacy. Modeling the predictive control with a weighted optimization of fuel consumption and nitrogen oxide emission is gaining increasing traction, especially in Europe.

We would like to thank all the authors for their excellent contributions and all the reviewers for their rigorous reviews and valuable comments. We also appreciate the strong and detailed support from the Editor-in-Chief Dr. Tarek El-Bawab, and from Jennifer Porcello and Joseph Milizzo of the publishing team.

BIOGRAPHIES

VUK MAROJEVIC (vuk.marojevic@msstate.edu) is an associate professor in electrical and computer engineering at Mississippi State University. He obtained his M.S. from the University of Hannover, Germany, in 2003 and his PhD from Barcelona Tech-UPC, Spain, in 2009, both in electrical engineering. His research interests are in 4G/5G security, spectrum sharing, software radios, testbeds, resource management, and vehicular and aerial communications technologies and systems.

CHARLES A. KAMHOUA (charles.a.kamhoua.civ@mail.mil) is a senior research engineer at the Network Security Branch of the U.S. Army Research Laboratory (ARL) in Adelphi, Maryland, where he is responsible for conducting and directing basic research in the area of game theory applied to cyber security. Prior to joining ARL, he was a researcher at the U.S. Air Force Research Laboratory, Rome, New York, for six years and an educator at different academic institutions for more than 10 years.

JEFFREY H. REED [F] (reedjh@vt.edu) is the founder of Wireless @ Virginia Tech, and served as its director until 2014. He is the Founding Faculty Member of the Ted and Karyn Hume Center for National Security and Technology. He founded several companies that develop spectrum sharing and cybersecurity technologies. Currently he serves as the interim director for the Commonwealth Cyber Initiative.

FRIEDRICH K. JONDRAL (Friedrich.Jondral@kit.edu) is a retired full professor who lives in Karlsruhe, Germany. From 1993 until 2015, he was the director of the Communications Engineering Lab at the Karlsruhe Institute of Technology. His main research areas are reliable and secure communications, dynamic spectrum access, software defined radio, cognitive radio, radar, and signal analysis.