Feature Topic to be published in the September 2019 Issue of IEEE Communications Magazine

Secure Wireless Communications for Vehicle-to-Everything

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 enable 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 scenarios and environmental conditions. This poses a stringent need for ultra-reliable and ultra-low latency communications in dense environments, where thousands of cars can be simultaneously present in a given area, moving at different speeds and following different trajectories.

Whereas two major vehicle-to-everything (V2X) protocols have already been standardized and some commercial products are already available, research is ongoing to make these systems more reliable and more secure for safety and efficiency critical V2X applications. Vehicular communications systems need to be secure and the services be resilient to attacks that can compromise the system's performance or the user or data privacy. In a multi-node and dynamic vehicular network, effective identification and authenticity of user is needed to enable authorized access to services or information as well as authorized provisioning of services or information. The integrity of messages is necessary to ensure that information is accurate and can be trusted. The availability of the service or information for safe and efficient traffic flow and the confidentiality and privacy of users, their data and actions from eavesdropping and exploitation. Likewise, non-repudiation and accountability of the source are needed to ensure the system is sustainable and can evolve.

This feature topic (FT) brings together researchers and practitioners in vehicular communications security to share their latest research contributions and expert insights. The interest of this FT is on all aspects on vehicular communications security including, but not limited to the following topics:

- V2X protocol security
- Authentication and accounting
- Physical layer techniques for increased security
- Security metrics
- Testbeds and measurement campaigns
- UAV communications security
- Standardization efforts
- Secure spectrum sharing
- Game theory for vehicular communications security
- Cyber deception in vehicular communications

Submission Guidelines

Manuscripts should conform to the standard format as indicated in the Information for Authors section of the Manuscript Guidelines[1]. Please, check these guidelines carefully since they have been updated recently.

All manuscripts to be considered for publication must be submitted by the deadline through Manuscript Central. Select the "September 2019/ Secure Wireless Communications for Vehicle-to-Everything" topic from the drop-down menu of Topic/Series titles.

Important Dates

Manuscript Submission Deadline: March 15, 2019
Final Manuscript Due: July 15, 2019
Decision Notification: June 15, 2019
Publication Date: September 2019

Guest Editors

Vuk Marojevic, Mississippi State University, US, vuk.marojevic@msstate.edu
Charles Kamhoua, Army Research Laboratory, US, charles.a.kamhoua.civ@mail.mil
Jeffrey H. Reed, Virginia Tech, US, reedjh@vt.edu
Friedrich Jondral, Karlsruhe Institute of Technology, Germany, Friedrich.Jondral@kit.edu

[1] https://www.comsoc.org/publications/magazines/ieee-communications-magazine/author-guidelines/manuscript-submission