CALL FOR PAPERS

IEEE Internet of Things Journal Special Issue on Security and Privacy of Intelligent Vehicles

Recent proliferation of artificial intelligence, machine learning, the Internet of Things (IoT), and edge-fog-cloud computing envisions that intelligent vehicles are capable of innovative solutions to change our lifestyles. Unavoidably the potential benefits come along with new challenges and concerns on security and privacy. For example, interconnection may provide interfaces for attackers to control systems or acquire confidential information, and systems may enter unsafe or catastrophic conditions if they are autonomous without human's interference. This special issue seeks research contributions on theoretical analysis, vulnerability discovery, novel system architecture construction and design, emerging applications, experimental studies, and social impacts of intelligent vehicles. The topics include but are not limited to:

- Accident prevention
- Adaptive attack mitigation for intelligent vehicles
- Authentication and access control for intelligent vehicles
- Availability, recovery, and auditing for intelligent vehicles
- Blockchain-based security and privacy solutions for vehicular applications
- Cooperative driving and traffic management
- Data security and privacy for intelligent vehicles
- Driver behavior analysis
- Electric vehicle charging systems' security and privacy
- Intrusion detection for intelligent vehicles
- Learning-based attacks and defenses for intelligent vehicles
- Malware analysis for intelligent vehicles
- Security-aware and privacy-aware system design
- Smart contract-based trustable and verifiable computations for vehicular applications
- Threat modeling for intelligent vehicles
- Traffic theory, modeling, and analysis
- Transportation systems' security and privacy
- V2V, V2I, and V2X: architectures and system design
- Vehicle information systems
- Vehicle-specific gateways and firewalls
- Vehicle-specific hardware security modules
- Vehicle-to-vehicle communication and in-vehicle communication
- Vulnerability analysis for intelligent vehicles

Important Dates:

- Submission Deadline: September 15, 2024
- First-Round Review Due: November 15, 2024
- Revision Due: December 15, 2024
- Second-Round Review Due (Notification): January 15, 2025
- Final Manuscript Due: January 31, 2025
- Publication Date: February 2025

Submission Guidelines:

The submission guidelines are available at http://ieee-iotj.org/guidelines-for-authors/. All manuscripts and revision must be submitted electronically through IEEE Manuscript Central, http://mc.manuscriptcentral.com/iot, with the selection " Special Issue on Security and Privacy of Intelligent Vehicles" for the type.

Guest Editors:

- Yu Chen, Binghamton University - State University of New York, NY, US (ychen@binghamton.edu)
- Chung-Wei Lin, National Taiwan University, Taiwan (cwlin@csie.ntu.edu.tw)
- Bo Chen, Michigan Technological University, MI, US (bchen@mtu.edu)
- Qi Zhu, Northwestern University, IL, US (qzhu@northwestern.edu)
- Weizhi Meng, Technical University of Denmark, Denmark (weme@dtu.dk)