Guest Editorial: Cyber-Physical Threats and Solutions for Autonomous Transportation Systems

THE rapid evolution of technology has radically changed our everyday lives from multiple points of view. Systems and devices are nowadays more interconnected and capable of taking autonomous decisions without or with limited human intervention. Among the others, transportation systems are populated by smart and interconnected vehicles that need to communicate with each other and with critical infrastructures to orchestrate traffic and mobility. Such vehicles are equipped with multiple modules, which are sensing or communication devices that help the vehicle in assessing its well-being besides providing the basic information to be shared for the orchestration in the overall network. Transportation systems are hence operated through multiple technologies that need to cooperate to provide efficient delivery of goods and human mobility, as well as to provide security in the overall network. The latter task is complicated by the fact that vehicles autonomously drive and cooperate in the network without human intervention. In fact, thanks to the self-regulating capacity of the modules deployed both inside each vehicle and in the network infrastructure, vehicles do not need to be actively and fully driven by humans as in the past but require minimum intervention to mitigate extreme cases. The level of human intervention depends on the specific architecture and solution but is generally very limited. The overall transportation network can be therefore represented by a cyber–physical system, where a large number of sensors, actuators, and multiple technologies are connected and exchange information.

To guarantee overall network security, attack detection and the design of suitable countermeasures play a fundamental role. In fact, although human intervention may be able to mitigate part of the attacks (e.g., a non-fully-autonomous vehicle envisioning the presence of a driver may allow for overriding the autonomous module and allow the driver to prevent detours/crashes), large and articulated systems may still be vulnerable to security and privacy threats. The security of cyber-physical systems has been widely studied in the literature. However, most of the proposed solutions target either cyber or physical threats, without providing a unified view to detect and mitigate more complicated attacks. Considering the increasing attackers' capabilities and resources, the research shall start focusing on more complicated and combined attacks, where an attacker not only has the technical knowledge to design the most powerful attack but also has the means to jeopardize the overall network security. Privacy also plays a fundamental role in these systems. In fact, the information exchanged in transportation networks shall not jeopardize the privacy of passengers or companies delivering goods. Therefore, viable solutions should not guarantee security at the price of privacy.

The purpose of this Special Section is to collect the latest research achievements in cyber–physical threats and countermeasures in autonomous transportation systems. We expect that this Special Section will provide the audience with a complete and detailed assessment of both models and solutions for security and privacy in autonomous transportation systems jointly considering both the cyber and physical points of view This will serve as a starting point for future research toward more secure and reliable autonomous transportation means.

A. BRIGHENTE, *Guest Editor*
University of Padova, Department
of Mathematics, 35121, Padua,
Italy

M. CONTI, *Guest Editor*
University of Padova, Department
of Mathematics, 35121, Padua,
Italy

R. POOVENDRAN, *Guest Editor*
Department of Electrical and
Computer Engineering, University
of Washington, 98195 Seattle,
USA

J. ZHOU, *Guest Editor*
School of Information Systems
Technology and Design, Singapore
University of Technology and
Design, 487372, Singapore

Date of current version 24 May 2023.
Digital Object Identifier 10.1109/TII.2023.3272248