Workshop title

Advanced Cybersecurity Approaches for connected, automated and electric vehicles

Workshop proposer(s)

Christos Alexakos*, Konstantinos Votis, Christos Laoudias, Evangelos Bekiaris, Georgios Ellinas, Antonios Lalas

Abstract

Modern vehicles require about 100 million lines of code, more than e.g., a Boeing 787 (14 million) or Facebook (61 million), transforming them to some of the most complex systems. The new capabilities increase dramatically the complexity of a vehicle's systems, and although these complex systems have significantly improved vehicle performance, the probability of impairments has also increased. The damaging effects of cyberattacks to the automotive industry can be tremendous. One can mention for example the damage in the reputation of vehicle manufacturers, the loss of working hours, increased environmental pollution due e.g., to intentional traffic jams, and ultimately the great danger for human lives, either they are drivers, passengers or pedestrians.

The aim of the Workshop is to bring together ITS engineers, researchers, and practitioners interested in key areas where cybersecurity innovations are mostly needed, including but not limited to i) Autonomous vehicles, ii) Internet of Vehicles (IoV), and iii) Electrical Charging stations. Participants are invited to present and discuss modern vehicle cybersecurity challenges and focus on methods that mitigate associated safety risks. Papers describing original novel work and advanced prototypes, systems and tools are encouraged. The workshop would provide a platform for evaluating new frontiers in both basic and industrial research, development, integration, standards, advance service provisioning, and user communities addressing cybersecurity challenges in connected, autonomous and electric vehicles.

Keywords

- Transportation Security
- ITS Policy, Design, Architecture and Standards
- Data Mining and Data Analysis

Topics of interest

- Cybersecurity Strategies
- Robust security of systems, component, and networks
- Threat Analytics
- Digital Forensics
- Validation of correctness and security for vehicle systems
- Automotive Security threats to cyber-physical systems;
- Security architecture, implementation, and management of intelligent vehicles

- Security Techniques and protocols for cooperative vehicles;
- Data communication security in networked embedded systems;
- Automotive collision prediction and avoidance in cyber world;
- Security mechanism for automotive motion planning in dynamic environments
- Practical security experiences and testbeds related with intelligent vehicles
- Automotive industrial experiences relevant to safety and security of IV