Special Issue on

Artificial Intelligence Security for Autonomous Systems

Call for Papers

The advancement of artificial intelligence (AI) technologies is permeating all aspects of autonomous systems and other fields, accelerating the development of unmanned manufacturing and autonomous driving, among others. Since the inception of unmanned aircraft with the first flight in 1916, autonomous systems have gained significant attention due to their capacity to autonomously execute tasks without human intervention, leading to their diverse applications across various domains. Autonomous systems refer to machines or devices equipped with essential data processing units, sensors, controls, communications, and computing systems, including unmanned aerial vehicles (UAVs), ground-based mobile robots/vehicles, surface/subsurface vehicles, satellites, and other unconventional structures. Concurrently, the development of autonomous systems technology is accompanied by vulnerabilities and threats, resulting in several security concerns during their widespread adoption. AI security, as the security analysis of autonomous systems based on AI technologies, facilitates the identification of security risks through the data generated by the systems, thereby enhancing their safety to achieve more advanced objectives. Nevertheless, due to the complexity of autonomous systems, vulnerabilities in communication networks, and external uncertainties, numerous challenging issues remain unresolved.

This special issue primarily focuses on artificial intelligence security for autonomous systems, addressing original ideas, novel methods, and new applications of AI in autonomous systems in the context of security. We are soliciting original contributions, from leading researchers and practitioners from academia as well as industry, which address a wide range of theoretical and application issues in AI security for autonomous systems. Topics for this special issue include, but are not limited to:

- AI-based attack modeling for autonomous systems
- Efficient and improved solution for AI-based attack detection for autonomous systems
- Applications of AI-based vulnerability analysis for autonomous systems
- AI-based data security and privacy for autonomous systems
- AI-based secure state estimation for autonomous systems
- Typical autonomous systems application for AI-based distributed robust/resilient control
- AI-based security algorithms and mechanisms for autonomous systems
- Experimental evaluation for AI-based security of autonomous systems

Important Dates

- Paper Submission Deadline: **November 1, 2024**
- Completion of the first-round review: February 1, 2025
- Completion of the second-round review: June 1, 2025
- Final manuscripts due: September 1, 2025
- Tentative publication date: December 2025

Guest Editors

- Hao Zhang, Tongji University, China, zhang_hao@tongji.edu.cn
- Zhijun Li, Tongji University, China, zjli@ieee.org
- Claudio Melchiorri, University of Bologna, Italy, claudio.melchiorri@unibo.it
- Huaicheng Yan, East China University of Science and Technology, China, hcyan@ecust.edu.cn

Paper Submission

All papers are to be submitted through the IEEE's Manuscript Central for Transactions on Automation Science and Engineering http://mc.manuscriptcentral.com/t-ase. Please select the Manuscript Category "Topic-Based Special Issue" under "Type" in Step 1 and this specific Special Issue in Step 6 of your article's submission process. **All manuscripts must be prepared according to the IEEE Transactions on Automation Science and Engineering publication guidelines** (http://www.ieee-ras.org/publications/t-ase). Please address inquiries to zhang_hao@tongji.edu.cn.