Security and Safety, Vol. 2, E2023032 (2023)
https://doi.org/10.1051/sands/2023032
sands.edpsciences.org

Security and Safety in Unmanned Systems

Editorial

Open Access

Preface: Security and safety in unmanned systems

Jian Sun[1,*], Youmin Zhang[2], Hong Chen[3], Mou Chen[4], and Qinglei Hu[5]

[1] *School of Automation, Beijing Institute of Technology, Beijing 100081, China*
[2] *Department of Mechanical Industrial and Aerospace Engineering, Concordia University, Quebec H3G 1M8, Canada*
[3] *College of Electronic and Information Engineering, Shanghai 201804, China*
[4] *College of Automation Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing 211106, China*
[5] *School of Automation Science and Electrical Engineering, Beihang University, Beijing 100191, China*

Received: 1 October 2023 / Accepted: 4 October 2023 / Published online: 6 December 2023

Citation Sun J, Zhang Y, Chen H et al. Preface: Security and safety in unmanned systems. Security and Safety 2023; **2**: E2023032. https://doi.org/10.1051/sands/2023032

An unmanned system is defined as an electro-mechanical system capable of exerting its power to perform designated missions with no human operator aboard. Thanks to the development of digital design (artificial intelligence, control, *etc.*) and robotics in recent years, unmanned systems are making a revolution as an emerging technology with many different applications in the military, civilian, and commercial fields such as autonomous driving, medicine and healthcare, deep space exploration, and national security and defense. Despite the advantages brought by using unmanned systems, the widespread application process is accompanied by a number of issues and accidents. In particular, the development of unmanned system technology is associated with vulnerabilities and threats, including external disturbances, faults, and cyber-attacks, which always lead to severe damage to critical infrastructures as well as significant economic loss. These facts motivate the need for effective mechanisms to defend against the risks and/or to mitigate the associated effect on physical entities, and more and more attention is being paid to security and safety in unmanned systems. Nonetheless, there remain many fundamental challenges that restrain unmanned systems from engaging in complicated and challenging tasks. Based on these observations, this special topic focuses on security and safety in unmanned systems for the industry and academia. There are a total of 8 papers finally accepted for publication after going through strict manuscript reviews and revisions. Topics of the papers cover a number of interesting research directions in security and safety in unmanned systems.

Haichuan Yang, Ziquan Yu, and Youmin Zhang [1] investigate an event-triggered resilient consensus control method for nonlinear multiple unmanned systems under periodic DoS attacks, and introduce a data-based state prediction method into a model-based controller scheme to deal with the DoS attacks. It is proved that the Zeno behavior can be excluded.

The paper by Yongxia Shi, Ehsan Nekouei, and Qinglei Hu [2] studies the secure motion control problem for micro-spacecraft systems, and develops a novel semi-homomorphic encrypted control framework, consisting of a logarithmic quantizer, two uniform quantizers, and an encrypted control law based on the Paillier cryptosystem. The proposed framework ensures the security of the exchanged data over the communication network of the spacecraft, even when communication channels are eavesdropped by malicious adversaries.

* Corresponding author (email: sunjian@bit.edu.cn)

Lei Shi, Zhen Chen, Yucheng Shi, Lin Wei, Yongcai Tao, Mengyang He, Qingxian Wang, Yuan Zhou and Yufei Gao [3] propose a novel model poisoning attack based on the momentum of historical information, where the attacker makes new malicious updates by dynamically crafting perturbations using the historical information in the local training. Thus, the testing accuracy of the global model can be indiscriminately reduced with minimal information.

A study of networked control systems subjected to periodic denial-of-service (DoS) attacks of varying intensity is presented by Xiao Cai, Kaibo Shi, Kun She, Shouming Zhong, Shiping Wen and Yuanlun Xie [4] An intelligent secure event-triggered controller is designed to ensure the secure operation of the system under DoS attacks, where a constrained optimization problem is formulated and solved to select the trigger threshold.

In the paper by Yonghua Peng, Guohuai Lin, Guangdeng Chen and Hongyi Li [5], a dynamic event-triggered formation control strategy is proposed for a category of human-in-the-loop stochastic nonlinear multi-agent systems with fullstate constraints. Moreover, the presented strategy can guarantee that all signals of the MASs are semi-globally uniformly and ultimately bounded in probability.

A systematic assessment of cyber-physical security is developed for the lanekeeping control (LKC) system of autonomous vehicles by Yulei Wang, An Huang, Fan Yang, Ning Bian, Jiazhi Zhang and Lulu Guo [6] A security criterion is investigated taking tracking performance, comfort and vehicle stability in account, and shown to be effective to analyze the impact of the cyber-attacks on commercial LKC system by hardware-in-the-loop experiments.

The paper by Biao Ma and Mou Chen [7] proposes an attainable-equilibrium-set-based safety fight envelope (SFE) calculation, and presents a prescribed performance protection control scheme for unmanned air vehicles under external disturbances. The proposed SFE protection controller combines the desired safety trajectory, backstepping method, higher-order disturbance observer design, and prescribed performance control technique. In particular, the closed-loop is verified to be stable.

Yanhui Zhang, Di Mei, Yong Xu, and Lihua Dou [8] propose an adaptive cooperative secure tracking controller of networked multiple unmanned systems subjected to false data injection attacks. A quantizer-based encoding mechanism is constructed to reduce the communication bandwidth between agents, and a new adaptive law is added to the decoder to overcome the effect of false data.

We hope that the papers in this special topic will be of value to academic research and engineering practice. Finally, we thank all the authors for their contributions to this special topic, and are grateful to all the editors and reviewers for their strong support and valuable assistance.

References

[1] Yang HC, Yu ZQ and Zhang YM. Event-triggered resilient consensus control of multiple unmanned systems against periodic DoS attacks based on state predictor. Secur Saf 2023; **2**: 2023017.
[2] Shi YX, Nekouei E and Hu QL. Secure motion control of micro-spacecraft using semi-homomorphic encryption. Secur Saf 2023; **2**: 2023018.
[3] Shi L, Chen Z, Shi YC et al. MPHM: Model poisoning attacks on federal learning using historical information momentum. Secur Saf 2023; **2**: 2023006.
[4] Cai X, Shi KB, She K et al. Communication security of autonomous ground vehicles based on networked control systems: The optimized LMI approach. Secur Saf 2023; **2**: 2023016.
[5] Peng YH, Lin GH, Chen GD et al. Dynamic event-triggered-based human-in-the-loop formation control for stochastic nonlinear MASs. Secur Saf 2023; **2**: 2023024.
[6] Wang YL, Huang A, Yang F et al. Systematic assessment of cyber-physical security of lane keeping control system for autonomous vehicles. Secur Saf 2023; **2**: 2023027.
[7] Ma B and Chen M. Safety flight envelope calculation and protection control of UAV based on disturbance observer. Secur Saf 2023; **2**: 2023020.
[8] Zhang YH, Mei D, Xu Y et al. Adaptive cooperative secure control of networked multiple unmanned systems under FDI attacks. Secur Saf 2023; **2**: 2023029.