

2024 第七届 IEEE 国际无人系统大会 特邀专题简介表

特邀专题名称

集群无人系统协同安全控制

组织者

1. 赵宇，教授，西北工业大学
2. 王博辉，教授，西安交通大学
3. 张栋，教授，西北工业大学
4. 张卓，教授，西北工业大学

个人简介



赵宇，西北工业大学，副教授、博导，毕业于北京大学，多次出访香港城市大学、加州大学河滨分校、皇家墨尔本理工大学等国内外知名高校。长期从事多智能体系统协同控制、优化相关研究工作，目前发表学术论文 100 余篇，其中 IEEE 会刊 40 余篇，IEEETAC 和 Automatica 等顶刊长文 3 篇；主持国家级科研项目 3 项，省部级项目多项；2017 年被评为陕西省高层次人才，2019、2022 年获陕西省自然科学优秀学术论文奖 2 项，2021 年陕西省研究生教育一等奖，2022 年第 16 届 IFAC 复杂系统国际学术会议（IFAC-LSS-2022）大会主席。



王博辉，西安交通大学，教授，博导，主要从事人工智能算法分布式应用安全、信息物理融合系统建模、调度、控制与优化等方面的研究及应用工作，王教授是 2023 年度全球前 2% 顶尖科学家和西安交通大学青年拔尖人才 A 类，并曾获中国电子学会优博，中国仿真学会优博，IEEE ICIT 2022 最佳论文奖，IEEE 杰出副编辑（2020）等多项荣誉，担任 Heliyon Engineering (Cell 出版集团综合刊物), IEEE Transactions on Systems, Man, and Cybernetics: Systems, IEEE Transactions on Aerospace and Electronic Systems 等多个学术刊物的副编辑 (Associate Editor) 或编委。



张栋，副教授，博士生导师，复杂系统控制与智能协同技术国防科技重点实验室客座教授，西北工业大学国防科技专家，某无人蜂群分系统副总师，中电集团长风电子科技有限公司高级顾问，担任集群智能与协同控制专业委员会委员、中国智能物联专业委员会委员，国际期刊 Journal of Engineering 副主编 (Associate Editor)、国内期刊无人系统技术、航空兵器、导航定位与授时青年编委、2019 年、2020 年 IEEE 国际无人系统大会 (IEEE ICUS 2019/2020) 大会专题主席，2020 年获得 IEEE 国际无人系统大会的最佳组织者。另外是国家自然科学基金信息学部函评专家以及 Aerospace Science and Technology、International Journal of Aerospace Engineering、中国航空学报中英文版、控制与决策、兵工学报等多个国内外期刊的审稿人。



张卓，男，博士，西北工业大学航海学院助理教授，硕导，民盟盟员。于 2010 年获得沈阳航空航天大学学士学位，分别于 2012 年和 2017 年获得哈尔滨工业大学硕士和博士学位，于 2016 年赴加拿大维多利亚大学进行联合培养，2017 年 9 月开始在西北工业大学航海学院工作，担任助理教授。主要从事集群协同控制、水下航行器编队控制、鲁棒控制等方面的研究工作。目前主持/参与多项国家自然科学基金项目，第一作者发表学术论文 20 余篇，包括控制领域权威期刊 IEEE TAC、Automatica、IEEE 汇刊等 10 余篇。担任国际期刊 Journal of Mechanical Science and Technology (SCI) 编委 (Associate Editor)，担任国际会议 28th International Symposium on Industrial Electronics 分会场主席。

特邀专题简介

近年来，集群无人系统在军事、民用、交通、海洋、灾害应急、农业、工业等领域都有广泛的应用，如军事侦察、目标追踪、搜索和救援、森林火情监测、线路管道检查等。多个无人系统通过信息交互和协同工作，可以实现更复杂、更高效的任务完成，提升整体系统的性能和效率。然而，随着无人系统数量的增加和应用场景的多样化，如何确保集群无人系统之间的协同工作安全成为近年来集群无人系统控制领域的研究热点之一。

集群无人系统的协同安全是指多个无人系统在执行任务时通过有效的协作与通信，确保整个系统在避障、路径规划、动作执行等方面能够相互配合、互相支持，以保障系统整体的安全性和效率。这其中涉及到隐私保护、攻击免疫，碰撞避免等多方面的问题与技术挑战：

- 集群无人系统协同隐私保护问题

在集群无人系统中，隐私保护问题是一个备受关注的议题。集群无人系统包括多个无人机、无人车辆或其他无人设备，它们通过互联网、传感器和通信技术相互连接，共同完成各类任务。然而，这种高度互联的环境也带来了一系列隐私保护方面的挑战，例如，1) 集群无人系统中的数据采集和共享可能涉及个人隐私信息；2) 集群无人系统的数据传输过程中存在被窃取或篡改的风险。为了解决集群无人系统中的隐私保护问题，需要采取一系列措施：如数据加密与匿名化，访问控制与权限管理，隐私保护技术研究等。隐私保护是集群无人系统发展过程中必须重视的问题，只有充分考虑隐私保护需求并采取相应措施，才能确保无人系统在安全可靠的前提下发挥其应用潜力。

- 集群无人系统协同攻击免疫问题

在实际应用中，集群无人系统可能面临多种类型的攻击，包括但不限于网络攻击、恶意软件攻击、物理破坏等。这些攻击可能导致系统瘫痪、数据泄露、信息篡改等严重后果。例如，在军事防御领域，网络攻击是应对无人机集群攻击的有效手段之一。无人机集群一旦遭受网络攻击，整个系统的协同将会被破坏，严重影响集群协同控制的安全性。集群无人系统的攻击免疫问题是指如何有效应对各种潜在的威胁和攻击，以确保系统的正常运行、数据的安全性和完整性。随着集群无人系统在各个领域的广泛应用，保障系统的安全性显得尤为重要。

- 集群无人系统协同避障问题

无人机、无人车在执行任务时可能会面临各种障碍和风险，如建筑物、树木、其他飞行器或车辆等。无人系统与障碍物发生碰撞，将造成设备损坏和环境破坏的风险，降低任务的完成效率和质量。因此，如何确保集群无人系统之间能够协同工作，避免碰撞和其他安全风险将成为无人系统研究的重要方向之

一。无人系统避障控制涉及到多个领域的技术背景知识，包括环境感知、障碍物检测与识别、路径规划算法、避障控制算法、自主导航系统以及机器学习与深度学习等。避障技术可以帮助无人系统避免与障碍物发生碰撞，这对于保护设备本身、避免事故发生以及减少意外损失都起到了重要作用，并保障了集群无人系统的安全运行。

IEEE ICUS 2024
Invited Session Summary

Title of Session

Cooperative Safety Control of Cluster Unmanned Systems

Organizers

1. Prof. Yu Zhao

Northwestern Polytechnical University, China

2. Prof. Bohui Wang

Xi'an Jiaotong University, China

3. Prof. Dong Zhang

Northwestern Polytechnical University, China

4. Prof. Zhuo Zhang

Northwestern Polytechnical University, China

Biosketches of Organizers



Yu Zhao, associate professor and doctoral supervisor of Northwestern Polytechnical University, graduated from Peking University, has visited City University of Hong Kong, University of California Riverside, Royal Melbourne Institute of Technology and other well-known universities at home and abroad for many times. He has been engaged in collaborative control and optimization of multi-agent systems for a long time, and has published more than 100 academic papers, including more than 40 IEEE journals and 3 long articles in IEEETAC and Automatica. He presided over 3 national research projects and many provincial and ministerial projects; In 2017, he was named as the high-level Talent of Shaanxi Province, won two outstanding Academic paper awards of Natural Science of Shaanxi Province in 2019 and 2022, the first prize of graduate Education of Shaanxi Province in 2021, and the chairman of the 16th IFAC International Academic Conference on Complex Systems (IFAC-LSS-2022) in 2022.



Bohui Wang, professor, PhD supervisor, Xi'an Jiaotong University, mainly engaged in the research and application of artificial intelligence algorithm distributed application security, information and physical fusion system modeling, scheduling, control and optimization, etc. Professor Wang is the world's top 2%

top scientist in 2023 and Xi 'an Jiaotong University Young Top Talent Class A, and has won the China Electronics Association outstanding doctorate. China Simulation Society Excellent Blog, IEEE 2022 Best Paper Award, IEEE Outstanding Associate Editor (2020) and many other honors, Heliyon Engineering(Cell Publishing Group comprehensive publication), IEEE Transactions on Systems, Man, and Cybernetics: Systems, IEEE Transactions on Aerospace and Electronic Systems and other academic journals Associate Editor or editorial board.



Dong Zhang, Associate Professor, doctoral supervisor, visiting professor of Complex System Control and Intelligent Collaborative Technology of National Defense Key Laboratory of Science and Technology, National defense science and technology expert of Northwestern Polytechnical University, Deputy chief engineer of an

unmanned swarm subsystem, senior consultant of CLP Group Changfeng Electronic Technology Co., LTD., member of Cluster Intelligence and Collaborative Control Professional Committee and member of China Intelligent Internet of Things Professional Committee. Associate Editor of the international Journal of Engineering, Young Editorial Board of the domestic journal Unmanned Systems Technology, Aviation Weapons, Navigation Positioning and Timing, 2019, 2020 IEEE International Unmanned Systems Conference (IEEE ICUS 2019/2020) Conference Thematic Chair, won the best organizer of the IEEE International Unmanned Systems Conference in 2020. In addition, he is a letter evaluation expert of the Information Department of the National Natural Science Foundation, Aerospace Science and Technology, and International Journal of Aerospace Reviewer for many domestic and foreign journals such as Engineering, Chinese and English edition of Aeronautical Journal of China, Control and Decision, Ordnance Engineering Journal.



Zhuo Zhang, male, Ph.D., Assistant professor, Master's supervisor, and member of China Democratic League, School of Navigation, Northwestern Polytechnical University. He received his bachelor's degree from Shenyang Aerospace University in 2010, master's degree from Harbin Institute of Technology in 2012

and Doctor's degree from Harbin Institute of Technology in 2017. In 2016, he went to Victoria University, Canada for joint training. In September 2017, he began to work at the Navigation School of Northwestern Polytechnical University as an

assistant professor. He is mainly engaged in the research of cluster cooperative control, underwater vehicle formation control, robust control and so on. At present, he has presided over/participated in a number of National Natural Science Foundation projects, and the first author has published more than 20 academic papers, including more than 10 authoritative journals in the field of control, such as IEEE TAC, Automatica, and IEEE Transactions. As an Associate Editor of the international Journal of Mechanical Science and Technology (SCI), Chair of the 28th International Symposium on Industrial Electronics.

Details of Session

In recent years, cluster unmanned systems have been widely used in various fields such as military, civil, transportation, maritime, disaster response, agriculture, and industry. Applications include military reconnaissance, target tracking, search and rescue, forest fire monitoring, and pipeline inspections. By enabling multiple unmanned systems to interact and work together, more complex and efficient tasks can be accomplished, enhancing the overall system performance and efficiency. However, with the increasing number of unmanned systems and diversification of application scenarios, ensuring the safety of collaborative work among cluster unmanned systems has become one of the hot research topics in the field of cluster unmanned system control.

The collaborative safety of cluster unmanned systems refers to the effective collaboration and communication among multiple unmanned systems during task execution, ensuring that the entire system can cooperate, support each other in obstacle avoidance, path planning, action execution, etc., to guarantee the overall system's security and efficiency. This involves various issues and technical challenges such as privacy protection, attack immunity, collision avoidance, among others:

- Collaborative Privacy Protection Issue in Cluster Unmanned Systems

Privacy protection is a highly concerning topic in cluster unmanned systems. These systems consist of multiple drones, unmanned vehicles, or other unmanned devices that are interconnected through the internet, sensors, and communication technologies to complete various tasks. However, this highly interconnected environment also brings a series of privacy protection challenges, such as: 1) data collection and sharing in cluster unmanned systems may involve personal privacy information; 2) there are risks of data theft or tampering during data transmission in

cluster unmanned systems. To address privacy protection issues in cluster unmanned systems, measures like data encryption and anonymization, access control and permission management, and privacy protection technology research are necessary. Privacy protection is a crucial aspect that must be considered in the development of cluster unmanned systems to ensure their application potential while maintaining security and reliability.

- Collaborative Attack Immunity Issue in Cluster Unmanned Systems

In practical applications, cluster unmanned systems may face various types of attacks, including but not limited to network attacks, malicious software attacks, physical destruction, etc. These attacks can lead to system paralysis, data leakage, information tampering, and other severe consequences. For example, in military defense, network attacks are an effective means to counter unmanned aerial vehicle cluster attacks. Once a drone cluster is subjected to a network attack, the coordination of the entire system will be disrupted, significantly affecting the security of cluster collaborative control. The issue of attack immunity in cluster unmanned systems refers to effectively addressing various potential threats and attacks to ensure the normal operation of the system, data security, and integrity. With the widespread application of cluster unmanned systems in various fields, ensuring the security of the system is particularly important.

- Collaborative Collision Avoidance Issue in Cluster Unmanned Systems

Unmanned aerial vehicles and unmanned vehicles may encounter various obstacles and risks during task execution, such as buildings, trees, other aircraft, or vehicles. Collisions between unmanned systems and obstacles can lead to equipment damage and environmental destruction, reducing task completion efficiency and quality. Therefore, ensuring that cluster unmanned systems can collaborate to avoid collisions and other safety risks will become an important direction of research in unmanned systems. Collision avoidance control for unmanned systems involves knowledge from multiple technical backgrounds, including environmental perception, obstacle detection and recognition, path planning algorithms, collision avoidance control algorithms, autonomous navigation systems, as well as machine learning and deep learning. Collision avoidance technology can help unmanned systems avoid collisions with obstacles, playing a crucial role in protecting equipment, preventing accidents, reducing unexpected losses, and ensuring the safe operation of cluster unmanned systems.