SCIENCE CHINA
Information Sciences

• PERSPECTIVE •

May 2024, Vol. 67, Iss. 5, 156201:1–156201:3
https://doi.org/10.1007/s11432-024-4001-6

Cooperative control for heterogeneous multi-agent systems: progress, applications, and challenges

Bing YAN[1], Peng SHI[1*] & Jonathon CHAMBERS[2]

[1]*School of Electrical and Mechanical Engineering, Faculty of Science, Engineering and Technology, The University of Adelaide, Adelaide* SA5005*, Australia;*
[2]*School of Engineering, College of Science and Engineering, University of Leicester, Leicester* LE1 7RH*, UK*

Received 22 January 2024/Accepted 21 February 2024/Published online 18 April 2024

Cooperative control for heterogeneous multi-agent systems (MASs) is a critical and rapidly evolving field in modern automation and robotics. Characterized by the integration of agents with diverse capabilities and functionalities, such as unmanned aerial and ground vehicles, these systems efficiently execute complex tasks through consensus in cyber-layer communication and physical layer operations [1]. Accordingly, advanced cooperative control methods are essential to ensure both cyber security—safeguarding against malicious attacks, and physical safety—operating reliably under physical faults and non-cooperative obstacles. As shown in Figure 1, this study explores the latest progress, various applications, and ongoing challenges in this field, emphasizing the importance of secure and safe cooperative control in heterogeneous MASs.

Progress. This study reviews the progress in heterogeneous MAS cooperation, secure control under cyber-attacks, and safe control under physical threats.

• Heterogeneous MAS cooperation. The cooperative control problems in heterogeneous MASs mainly revolve around two key aspects: consensus and formation control.

Consensus. The fundamental problem of heterogeneous MASs is output consensus problem [2]. A heterogeneous MAS can be modeled as

$$\dot{x}_i = f_i(x_i, u_i), \quad y_i = h_i(x_i, u_i), \quad i = 1, 2, \ldots, n, \qquad (1)$$

where $x_i \in \mathbb{R}^{n_i}$ and $u_i \in \mathbb{R}^{m_i}$ represent the states and inputs of the ith agent, and f_i and h_i are sufficiently smooth nonlinear functions. Despite the differences in state orders n_i and dynamics (f_i, g_i) of each agent, various agents can output their common interest variables $y_i \in \mathbb{R}^p$ to realize output consensus. A framework based on output regulation control has been proposed for consensus [2], and a common reference exosystem is modeled for heterogeneous agents to track as $\dot{v} = f_i^v(v),\ y_v = h_i^v(v)$, where $v \in \mathbb{R}^{n_0}$ and $y_v \in \mathbb{R}^p$ are the exosystem's inputs and outputs. f_i^v and h_i^v are the system's dynamics and output functions. As the exosystem is generally not accessible to all agents, the framework involves a distributed exosystem observer at the cyber layer as

$$\dot{\hat{v}}_i = O_i(\hat{v}_i, u_i^v(\phi_i)),\ \phi_i = \sum_{j=0}^{n} a_{ij}\left(\hat{v}_i - \hat{v}_j\right),\ \hat{v}_0 = v, \qquad (2)$$

where $\hat{v}_i$ is the observed value of v and ϕ_i is the cooperative error. a_{ij} is an element of the adjacency matrix for agent communication, where the exosystem is indexed as 0. The observer dynamic function O_i and the control input $u_i^v(\phi_i)$ are designed based on Lyapunov stability theory to ensure that the convergence of the observation error $e_i^v = \hat{v}_i - v$. Then, an output consensus controller for heterogeneous MAS (1) is designed as

$$u_i = k_i(x_i, z_i),\ \dot{z}_i = g_i(z_i, \hat{e}_i^v),\ \hat{e}_i^v = y_i - h_i^v(\hat{v}), \qquad (3)$$

where z_i represents a dynamic compensation variable and g_i defines its nonlinear system dynamics function, which involves the internal model information [1,3] of the exosystem. The design of the control function k_i is based on Lyapunov stability theory to ensure the convergence of the observer-based output error $\hat{e}_i^v$. Under observer (2) and controller (3), the convergence of the consensus output error $e_i = y_i - y_v$ can be achieved. However, the inevitable exchange of information between individuals is subject to various malicious cyber-attacks, presenting a significant challenge to the communication security of heterogeneous MASs.

Formation control. Formation control is a strategy to arrange agents in a predetermined structure and maintain the desired spatial relationships among them. It is extended from the output consensus problem of heterogeneous MASs with additional consideration of a reference time-varying formation (TVF) system as $\dot{x}_i^f = f_i^f(x_i^f),\ y_i^f = h_i^f(x_i^f)$, where $x_i^f \in \mathbb{R}^{n_i^f}$ and $y_i^f \in \mathbb{R}^p$ are the inputs and outputs of the ith TVF system. f_i^f and h_i^f represent its system dynamic and output functions. Similarly, the design of the observer at the cyber-layer is consistent with (2), and the output controller for formation control at the physical layer is designed as

$$u_i = k_i(x_i, z_i),\ \dot{z}_i = g_i^f(z_i, \hat{e}_i^f),\ \hat{e}_i^f = y_i - h_i^v(\hat{v}) - y_i^f, \quad (4)$$

where the system function g_i^f of compensation variable z_i involves the internal model information of the exosystem and TVF [1, 3]. Design u_i such that the observer-based formation output error $\hat{e}_i^f$ converges, combining observer (2) to ensure the convergence of the formation output error $e_i = y_i - y_v - y_i^f$. However, during the formation process, unknown non-cooperative obstacles in dynamic environments

* Corresponding author (email: peng.shi@adelaide.edu.au)

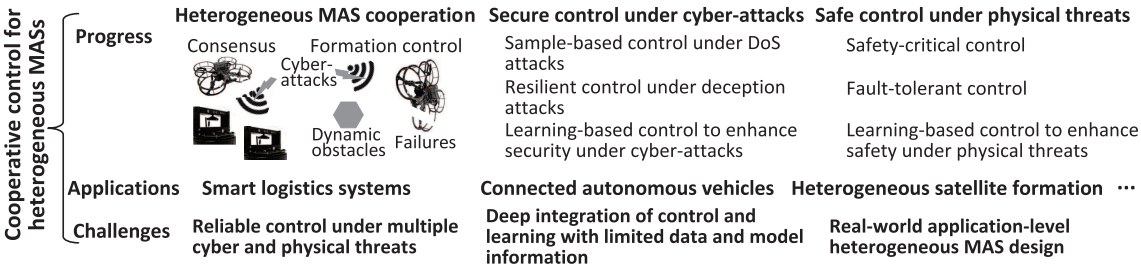

Figure 1 Cooperative control of heterogeneous MASs.

and inevitable physical failures present challenges. Ensuring system safety in the face of these physical threats is crucial for the efficiency of collaborative task completion.

• Secure control under cyber-attacks. The communication networks of MASs are vulnerable to cyber-attacks, such as typical attacks like denial of service (DoS) and deception attacks. Secure control methods have been intensively investigated for these attacks, and learning-based approaches have been studied to enhance system security.

Sample-based control under DoS attacks. DoS attacks are malicious attempts to jam communication between agents. Sample-based control strategies, such as event-triggered observers, become crucial in facing DoS attacks in heterogeneous MASs [4]. These strategies manage the system using condition-based sampled communication interactions. The effectiveness of this method against DoS attacks results from its reduced communication frequency, thereby decreasing the system's vulnerability to these attacks. The sampling rate must be carefully calculated based on event-triggered conditions related to the cooperative error to maintain system performance without compromising security [4]. However, these methods require prior knowledge of the model information of MASs and DoS attacks. There remains a significant challenge when model information is inadequate.

Resilient control under deception attack. Deception attacks involving injecting misleading information into the communication channels between agents, pose a substantial security risk in MASs. Resilient control strategies have been extensively studied for identifying and mitigating the impacts of these attacks. These strategies often utilize advanced estimators or detection algorithms to identify deception attacks. Then, the system can either transition to a secure operational mode to retain control or employ compensators to mitigate the impact of the attack. A remarkable approach has been proposed to observe the leader's status and offset the unmatched disturbances arising from deception attacks [5]. This approach is designed to achieve leader-following consensus within a predefined time, which is crucial for enabling MASs to quickly recover and continue functioning effectively under attacks. However, these model-based secure methods of MASs have limited resilience against deception attacks.

Learning-based control to enhance security under cyber-attacks. Utilizing machine learning in the controller design of heterogeneous MASs significantly strengthens their defense against cyber-attacks without adequate model information. Learning-based control enables agents to predict potential security risks and adaptively alter control protocols to counter these cyber-attacks. For instance, a data-driven algorithm has been developed to learn and adjust controller parameters, progressively enhancing the system's ability to tackle new and evolving security threats [6]. Learning-based secure control methods improve long-term resilience and robustness, ensuring a reliable network environment for heterogeneous MASs.

• Safe control under physical threats. Next, we focus on safe control methods for heterogeneous MASs under non-cooperative obstacles and physical faults, and learning-based control methods to enhance physical security.

Safety-critical control for obstacle avoidance. Safety-critical control refers to a strategy ensuring that the operations within MASs are performed without compromising safety, even under challenging or unexpected conditions. Similar to control Lyapunov functions (CLF), this approach defines the system's safe set using control barrier functions (CBF) [7]. For example, CBF can be defined based on the distance between the agent and non-cooperative obstacles [3]. Methods based on CBF-CLF-QP (quadratic program) guarantee the stability of cooperative MASs while also ensuring that the agents converge within a safe domain without collisions. However, this method is sensitive to the system model information. The QP problem, solved under the safety conditions of CBF, may fail to guarantee system safety due to uncertain MASs and environments. Therefore, model-free approaches are needed to ensure system safety.

Fault-tolerant control. Fault-tolerant control systems are essential for maintaining the operational integrity of heterogeneous MASs in the event of physical failures, such as sensor/actuator faults [6] and communication link failures [4]. These systems are designed to detect and diagnose faults in real time and adapt the consensus or formation control strategies accordingly to tolerate these failures. Adaptations may include redistributing tasks among operational agents or modifying control parameters to maintain ongoing stability. The primary objective of fault-tolerant control is to ensure that MASs, despite individual agents' component failures, remains operational and achieves system performance and safety objectives. However, the magnitude and types of faults can vary in real time, and achieving accurate real-time fault detection, isolation, and control under multiple dynamic failures is challenging.

Learning-based control to enhance safety under physical threats. Integrating learning into control strategies can effectively enhance the safety of uncertain heterogeneous MASs, especially in unknown dynamic environments and unpredictable physical failures. This approach utilizes machine learning algorithms to augment the system's ability to anticipate and respond to the complexities and uncertainties of different environments and unexpected scenarios. By processing historical data and real-time operational feedback, learning-based controllers can recognize patterns, adapt to novel situations, and make more informed decisions. For instance, reinforcement learning-based safety-critical control methods have been proposed, combining CBF to avoid collisions for uncertain heterogeneous MASs

under non-cooperative obstacles [3]. A data-driven method is also being explored to tolerate link failures [4] when model information is insufficient. These methods are particularly beneficial in settings where conventional control approaches are inadequate due to the variability and unpredictability inherent in real-world conditions. Continuously evolving, learning-based control systems progressively enhance their ability to predict and mitigate safety risks, thereby improving the overall safety of heterogeneous MAS operations in various challenging scenarios.

Applications. Heterogeneous MASs have a wide range of applications in practice, including smart logistics systems, autonomous connected vehicles, and heterogeneous satellite formations.

• Smart logistics systems. Heterogeneous MASs find significant applications in smart logistics, where they can streamline and optimize the supply chain and distribution processes [8]. In such systems, different types of agents, including drones, autonomous ground vehicles, and robotic arms, work collaboratively. Drones can be used for aerial surveillance and parcel delivery, ground vehicles for transportation of goods, and robotic arms for warehousing operations. This collaboration enables efficient handling and transportation of goods, real-time tracking of inventory, and quick response to changing logistics needs. The integration of learning and control technologies in these agents further enhances the cooperation processes, making logistics operations more secure, safe, and efficient.

• Connected autonomous vehicles. Connected autonomous vehicles are a typical example of heterogeneous MASs in the transportation sector. This system involves various types of autonomous vehicles such as cars, buses, and trucks communicating and coordinating with each other to improve traffic flow, increase security and safety, and reduce congestion [9]. These vehicles share information about traffic conditions, road hazards, and operational status, allowing them to make coordinated decisions. Connected autonomous vehicles can drive in close formations, significantly improving fuel efficiency and road capacity.

• Heterogeneous satellite formation. The heterogeneous satellite formation involves a group of satellites with different capabilities and functions operating together in space. For example, a bipartite consensus control method based on leaderless and leader-following has also been developed for satellite formations [10]. By working in a coordinated manner with dynamic formations, these satellites can perform complex tasks such as detailed Earth observation, space exploration, and telecommunications relay more effectively than a single satellite. The objective of controllers is to maintain the formation and ensure communication consensus in the harsh and variable conditions of space.

Challenges. Although significant progress has been made in cooperative control for heterogeneous MASs, there remain several challenges to overcome that require future research in the following areas.

• Reliable control under multiple cyber and physical threats. One of the primary challenges in heterogeneous MAS cooperation is ensuring reliable control in the presence of various threats. When both cyber and physical threats are present simultaneously, it is very difficult to ensure real-time threat detection and reliable control. The diversity of agents in heterogeneous MASs further complicates this issue. Developing secure and safe control strategies that can adapt to these diverse threats and ensure efficient operation deserves further study.

• Deep integration of control and learning with limited data and model information. Another challenge lies in the deep integration of control strategies and machine learning techniques, especially when working with limited data and incomplete models. This integration is complex, as learning algorithms must efficiently handle sparse data and limited model information while maintaining system stability and reliability. Therefore, the deep integration of control and learning strategies is one of the important future directions in the research of heterogeneous MASs.

• Real-world application-level heterogeneous MAS design. Frequent occurrences of multi-drone formation failures and autonomous vehicle collision incidents indicate that designing reliable heterogeneous MASs is very difficult for real-world applications. Further research is needed at the application-level system design to integrate different types of agents in challenging environments and accomplish various complex tasks. Ensuring security, safety, efficiency, and flexibility in such systems is crucial for their successful deployment in real-world scenarios.

Conclusion. This study provides an overview of the advancements, applications, and challenges in the field of heterogeneous MASs with a focus on cooperative control. It summarizes the existing secure control methods under cyber-attacks and safe control approaches in physical threats. Additionally, we discuss the potential applications of heterogeneous MASs and future research directions to address remaining challenges. We hope that this work can inspire researchers studying cooperative control of heterogeneous MASs.

Acknowledgements This work was partially supported by Australian Research Council (Grant No. DP240101140).

References

1 Shi P, Yan B. A survey on intelligent control for multiagent systems. IEEE Trans Syst Man Cybern Syst, 2021, 51: 161–175
2 Wu Y, Zhang H, Wang Z, et al. Output consensus of heterogeneous linear multiagent systems with directed graphs via adaptive dynamic event-triggered mechanism. IEEE Trans Cybern, 2023, 53: 4606–4618
3 Yan B, Shi P, Lim C P, et al. Security and safety-critical learning-based collaborative control for multiagent systems. IEEE Trans Neural Netw Learn Syst, 2024. doi: 10.1109/TNNLS.2024.3350679
4 Yang Y, Li Y F, Yue D. Event-trigger-based consensus secure control of linear multi-agent systems under DoS attacks over multiple transmission channels. Sci China Inf Sci, 2020, 63: 150208
5 Ni J, Zhao S, Cao J, et al. Predefined-time consensus tracking of high-order multiagent system with deception attack. Inf Sci, 2023, 649: 119671
6 Deng C, Gao W, Wen C, et al. Data-driven practical cooperative output regulation under actuator faults and DoS attacks. IEEE Trans Cybern, 2023, 53: 7417–7428
7 Chen Y, Singletary A, Ames A D. Guaranteed obstacle avoidance for multi-robot operations with limited actuation: a control barrier function approach. IEEE Control Syst Lett, 2021, 5: 127–132
8 Zhang M, Pan C. Hierarchical optimization scheduling algorithm for logistics transport vehicles based on multi-agent reinforcement learning. IEEE Trans Intell Transp Syst, 2023. doi: 10.1109/TITS.2023.3337334
9 Ma N, Li D Y, He W, et al. Future vehicles: interactive wheeled robots. Sci China Inf Sci, 2021, 64: 156101
10 Zhao G, Cui H, Hua C. Hybrid event-triggered bipartite consensus control of multiagent systems and application to satellite formation. IEEE Trans Automat Sci Eng, 2023, 20: 1760–1771