Frontiers in Computing and Intelligent Systems
ISSN: 2832-6024 | Vol. 12, No. 1, 2025

Research on UAV Formation Control under Deception Attacks

Minghui Xie [1, 3], Hongwei Ren [1, 2, *]

[1] College of Automation, Guangdong University of Petrochemical Technology, Maoming, Guangdong, China
[2] Guangdong Provincial Key Laboratory of Petrochemical Equipment Fault Diagnosis Maoming, Guangdong, 525000, China
[3] College of Information and Control Engineering, Jilin Institute of Chemical Technology, Jilin Jilin, 132022, China

*** Corresponding author:** Hongwei Ren

Abstract: With the rapid development of UAV technology and the continuous expansion of application scenarios, UAV formation control has become an important research direction in multi-agent systems. However, in complex network environments, deception attacks pose a serious threat to the security and stability of UAV formations. This paper systematically reviews the current research status of UAV formation control under deception attacks, providing an in-depth analysis from multiple dimensions, including research background, technical challenges, control methods, and security defenses. First, the development history and key technologies of UAV formation control are introduced. Then, the characteristics of deception attacks and their impact on formation control are analyzed in detail. Finally, the challenges faced by current research and future development directions are summarized.

Keywords: UAV Formation Control; Deception Attacks; Network Security; Multi-agent Systems.

1. Introduction

1.1. Research Background

In recent years, Unmanned Aerial Systems (UAS) technology has shifted from single-agent autonomous control to multi-agent collaborative control. According to the latest market analysis report by Grand View Research, the global drone market has grown from approximately $60 billion in 2020 to $73.06 billion in 2024, with an expected compound annual growth rate of 14.3% between 2025 and 2030, projecting the market size to reach $163.6 billion by 2030 [1]. This significant growth stems not only from the diversification of drone applications but also reflects the evolution of system architectures from centralized to distributed. UAV formation, as a typical collaborative mode of Multi-Agent Systems (MAS), integrates distributed control algorithms, consensus protocols, and swarm intelligence theory to achieve cooperative perception, decision-making, and execution of complex tasks, resulting in qualitative breakthroughs in system fault tolerance, task efficiency, and environmental adaptability [2].

The core scientific challenge in UAV formation control lies in achieving state consensus and adaptive collaborative control among multiple UAV nodes. From the perspective of control architecture evolution, Chen et al. [3] noted that current UAV formation control is rapidly transitioning from centralized to distributed architectures, with gradual advancements toward hybrid and self-organizing architectures. In centralized architectures, control decisions are computed and issued by a central processing unit, posing risks of single-point failures and communication bottlenecks. In contrast, distributed architectures enable UAV nodes to make autonomous decisions based on local state information and limited communication resources, demonstrating higher system flexibility and fault tolerance [4]. This theoretical paradigm shift arises from significant progress in networked control system theory, particularly the rigorous mathematical foundation provided by multi-agent collaborative control theory based on algebraic graph theory [5]. Liu et al. [6] made a breakthrough by proposing a sliding-mode control-based UAV formation method, effectively addressing robust formation control under communication constraints.

In practical applications, UAV formation technology has demonstrated significant value in both military and civilian domains. In the military field, swarm intelligence-based collaborative reconnaissance and precision strikes have become key research directions. Zhao et al. [7] developed a multi-agent game reinforcement learning model for UAV intelligent attack strategy generation, significantly enhancing combat effectiveness in complex environments. In the civilian sector, Sarhan et. al. classify formation control strategies into leader-follower, virtual structure, and behavior-based approaches, providing a framework for understanding the various methodologies employed in UAV formation control. This classification is essential for identifying the most suitable strategies for specific civilian applications. Kamel et. al. highlight the advancements in cooperative navigation and formation flight, particularly through the use of vision processing and radiofrequency data transmission. The low cost and operational flexibility of UAVs make them increasingly attractive for civilian applications, especially in areas that are hazardous for human pilots.; Pan et al. [10] proposed an improved artificial potential field method to address path planning and formation control for multi-UAV systems. In commercial applications, UAV formation delivery in logistics has improved efficiency by over 250% compared to traditional methods, while agricultural UAV formations have boosted operational efficiency in large-scale precision pesticide application by 300%–500%, significantly reducing labor costs and environmental impact [11].

As UAS networking and autonomous intelligence levels continue to rise, security threats have evolved from traditional physical-layer interference to more covert and destructive information-layer attacks [12]. According to the 2023 Global Intelligent Systems Security Report* by cybersecurity firm

Check Point, cyberattacks targeting UAS grew at an annual rate of 83.6% between 2018 and 2023, with deception attacks increasing from 31.2% to 57.8%, becoming the predominant attack vector [13].

Deception attacks are a class of advanced cyber threats based on information manipulation, where attackers inject carefully crafted false data or tamper with normal information flows to induce systems to make decisions based on erroneous information [14]. Depending on the target, deception attacks in UAV systems primarily manifest in three forms: (1) Positioning system spoofing (e.g., GPS/BeiDou spoofing), which disrupts UAV spatial perception by broadcasting forged navigation signals; (2) Communication channel spoofing, such as man-in-the-middle attacks or packet modification targeting peer-to-peer UAV communication links; and (3) Sensor data spoofing, which interferes with data streams from environmental sensors like cameras or LiDAR [15].

For UAV formations, cybersecurity faces even greater challenges. Liu et al. [16] systematically analyzed that distributed formation control systems exhibit significant cascading vulnerabilities. Specifically: First, compared to single-UAV systems, the multi-node nature of formations substantially expands the attack surface, allowing attackers to compromise the entire system by breaching any node's security. Second, based on network topology theory, the dependency of information propagation among nodes provides pathways for attack diffusion, enabling rapid spread through network connections. Third, the distributed decision-making mechanisms commonly used in formations heavily rely on information consensus; if critical nodes are spoofed, it may trigger chain reactions leading to systemic collapse [17]. Yin et al. [18] recently proposed an event-triggered sliding-mode control method incorporating an observer mechanism, which maintains formation stability under replay attacks. Simulations show this method confines attack impacts within predefined thresholds. Additionally, Xiao et al. [19] developed an improved sliding innovation sequence algorithm that successfully detected and isolated deception attacks on quadrotor UAVs in experiments, offering a new technical approach to enhance formation security.

UAV formation control faces multidimensional technical challenges under deception attacks. From a real-time control perspective, distributed formations impose strict constraints on communication and sensing timeliness and integrity, while security mechanisms introduce additional verification overhead, creating a "security-real-time trade-off" dilemma [20]. From an attack impact standpoint, deception attacks can exploit the topology-dependent nature of consensus protocols—even targeting a few critical nodes may destabilize the entire formation. From a defense strategy angle, traditional fault-tolerant control theories assume random failures, whereas deception attacks, as adversarial disturbances with intent and adaptability, exhibit intelligence and stealth that render existing defenses ineffective [21].

Current research has two notable gaps: From a control theory perspective, mainstream formation control algorithms (e.g., graph-based consensus or leader-follower approaches) often assume ideal communication environments, lacking inherent defenses against malicious spoofing. From a security theory perspective, existing studies typically treat attack detection and control reconfiguration as separate issues.

At the national strategic level, China's 14th Five-Year Plan explicitly prioritizes "secure autonomous control of unmanned intelligent equipment" as a key frontier technology [22]. The "14th Five-Year Plan for Smart Manufacturing Development" issued by the Ministry of Industry and Information Technology in 2022 further emphasizes the urgency of enhancing unmanned systems' reliability in complex adversarial environments [23]. The Ministry of Science and Technology's "New Generation AI" major project also identifies "secure autonomous unmanned systems" as a priority. Moreover, the "China UAV Development Report (2023) " highlights that cybersecurity attacks on UAV systems have become a major bottleneck limiting their critical applications [24]. The intersection of these national strategic needs and technological challenges forms the core academic motivation for this research.

1.2. Research Significance

This study focuses on the UAV formation control problem under deception attacks, holding multifaceted significance:

Theoretical Perspective: By integrating cybersecurity theory with distributed control theory, this study constructs a dynamic model of UAV formation under deception attacks, enriching the theoretical framework of secure networked control systems. This is particularly evident in the co-design of attack identification and robust control.

Technical Perspective: The proposed anti-deception attack formation control strategy will enhance the survivability and mission reliability of UAV systems in complex adversarial environments. The related technologies can effectively mitigate system risks posed by security threats and improve the operational value of the equipment.

Application Perspective: With the widespread use of UAV formations in civilian fields such as urban logistics and emergency rescue, the findings of this study will directly promote the safe deployment and industrialization of UAV technology. Research on UAV formation control under deception attacks not only explores cutting-edge academic challenges but also responds to national strategic needs and industrial development requirements. The outcomes will provide theoretical foundations and technical safeguards for building safer and more reliable intelligent unmanned systems.

2. Research Status of UAV Formation Control

This section systematically reviews domestic and international research on UAV formation control technology advancements, cybersecurity research trends, spoofing attack theory and technology, and the latest progress in UAV formation control under deception attacks. It analyzes the strengths and weaknesses of existing studies to lay the foundation for this paper's research [25].

UAV formation control technology originated in the late 1990s, stemming from theoretical breakthroughs in Multi-Agent Systems (MAS) research [26]. In the early 21st century, with declining hardware costs and improved computational capabilities, UAV formation control gradually evolved from centralized architectures to distributed architectures [27]. Centralized control relies on a central processing unit for unified decision-making, while distributed control allows individual UAVs to make autonomous decisions based on local information, offering greater scalability and fault tolerance [28]. Existing research methods can be categorized as follows: consensus-based control, leader-follower

approaches, distributed control and consensus protocols, fault-tolerant control (FTC), and robust control strategies.

Consensus-Based UAV Formation Control is a method that coordinates information sharing and decision-making among UAVs to achieve collective behavioral consistency. This approach emphasizes mutual communication and feedback among UAVs in dynamic environments to reach a unified state or objective, thereby enhancing overall formation performance and collaborative efficiency. While this strategy focuses on individual behavioral norms, it prioritizes group synergy, demonstrating greater flexibility and adaptability in handling complex tasks and unexpected events. However, existing consensus control algorithms often fail to maintain formation stability and consistency under communication deception attacks, highlighting the urgent need for more robust control mechanisms to improve interference resistance in adverse environments. Relevant studies include: Xu et al. [29] investigated consensus-based formation control for multi-UAV systems, designing a consensus protocol for strongly connected topologies using algebraic graph theory and backstepping techniques. Their results were extended to directed topologies, with simulations validating the method's effectiveness. Similarly, Kuriki et al. [30] proposed a consensus-based cooperative formation control strategy incorporating collision avoidance via artificial potential fields, ensuring convergence even when both formation control and collision avoidance algorithms are active.

Leader-Follower-Based UAV Formation Control is a strategy where a leader UAV serves as a reference point, and follower UAVs dynamically adjust their states and positions accordingly. This method emphasizes the leader's guiding role, ensuring followers maintain relative positions and speeds while flexibly responding to environmental changes and mission requirements, thereby achieving efficient coordination and stability. Relevant studies include: Yuan et al. [31] adopted a leader-follower approach using a data-driven model-free adaptive controller for trajectory tracking. The leader UAV employed an error-sign-based robust integral controller, while follower UAVs used an improved sliding mode control (ISMC) strategy for cooperative formation control. This method eliminated reliance on UAV mathematical models and demonstrated high control accuracy and robustness in simulations. Ranjan et al. [32] proposed a flexible formation scheme where follower UAVs maintain fixed relative distances but adjust their orientations based on the leader's maneuvers, enhancing tactical advantages.

Distributed Control and Consensus Protocol-Based UAV Formation Control decentralizes decision-making to individual UAVs, enabling global consistency through local information and collaborative mechanisms. This approach relies on inter-UAV communication and state sharing, ensuring each UAV can make independent decisions without centralized command, thereby enhancing system robustness and flexibility. Numerous studies have explored various methods and algorithms to improve formation efficiency and reliability in dynamic environments. Liu et al. [33] advanced the field by developing a formation obstacle-avoidance strategy based on consensus control and graph theory. Their leader-follower model, incorporating an improved artificial potential field method, allowed the leader UAV to avoid obstacles while navigating toward targets. The consensus protocol ensured formation maintenance even under disturbances, underscoring the importance of consensus protocols for stability in complex environments. Recent research has focused on distributed cooperative obstacle avoidance and formation reconfiguration. Literature [34] investigated distributed formation reconfiguration control based on consensus theory, enabling UAVs to dynamically adjust formations in response to environmental changes—a critical capability for maintaining operational effectiveness in rapidly changing real-world scenarios.

FTC-Based UAV Formation Control aims to enhance system stability and performance when components fail or are under attack. By designing redundancy mechanisms and adaptive algorithms, this strategy enables UAVs to swiftly adjust control policies in the face of faults or external interference, ensuring continuous operation and mission success. Research progress in FTC-based UAV formation control has proposed innovative solutions to challenges in maintaining formation integrity under faults and disturbances. For emergency medical rescue scenarios, Song et al. [35] developed a topology control algorithm to enhance fault tolerance in UAV networks. Their FTLMF algorithm constructed a doubly connected fault-tolerant network, significantly improving connection retention rates under node mobility, highlighting the critical role of network topology in formation resilience. Zhen et al. [36] studied fault-tolerant time-varying formation tracking control for UAV swarms with switching topologies. Their findings showed that well-designed formation tracking protocols allow followers to maintain desired formations while adapting to leader trajectories despite actuator faults, emphasizing the necessity of dynamic characteristics and robust control strategies. Literature [37] focused on fault-tolerant active disturbance rejection control (ADRC) for multirotor UAVs, addressing actuator faults and external disturbances like wind. By combining ADRC with spatiotemporal radial basis function neural networks, this study demonstrated practical approaches for maintaining stability in fluctuating environments using advanced control techniques.

Formation control of UAVs based on robust control strategies is a method aimed at enhancing the adaptability and stability of the system in the face of uncertainties and external disturbances. By incorporating robustness analysis and design principles, this strategy ensures that UAVs maintain structural integrity and operational efficiency in various complex environments, effectively addressing dynamically changing mission requirements and environmental challenges. Robust control strategies focus on preserving system stability under adversarial conditions, including methods such as "sliding mode control", "adaptive control", "H∞ control", and "feedback linearization".

Sliding Mode Control is a robust control technique that effectively handles uncertainties and disturbances. It forces the system's trajectory onto a predefined sliding surface, ensuring stability and performance even in the presence of model uncertainties and external disturbances. Xiang et al. [38] proposed a decentralized adaptive full-order sliding mode control framework for synchronized formation motion of multiple UAVs affected by system uncertainties. This framework integrates robust adaptive techniques to handle unknown bounded uncertainties without prior knowledge of their bounds. Fei et al. [39] developed a sliding mode neural observer to estimate nonlinear uncertainties in UAV models and designed sliding mode controllers for both position and attitude loops.

Adaptive Control techniques adjust controller parameters online to compensate for uncertainties and variations in

system dynamics. These methods are particularly useful when UAV parameters are unknown or time-varying. Reference [40] addressed the robust formation tracking problem for heterogeneous multi-robot systems, using radial basis function neural networks to approximate the uncertain dynamics of unmanned surface vehicles tracked by UAVs. Yang et al. [41] proposed a hybrid iterative learning formation control strategy that leverages historical input-output data to update current control inputs, enhancing robustness against dynamic model switching behaviors and external disturbances.

H∞ Control is a robust design method aimed at minimizing the impact of disturbances on system performance. Raffo et al. [42] introduced a nonlinear H∞ controller for quadrotor UAVs transporting payloads, ensuring swing-free load motion path tracking despite parameter uncertainties and disturbances. They also employed Lyapunov redesign techniques to reduce payload oscillations.

Feedback Linearization transforms nonlinear systems into linear ones, enabling the application of linear control methods. Hu et al. [43] proposed a distributed formation control architecture for trirotor UAVs, using robust feedback linearization to handle highly coupled and nonlinear dynamics, followed by a distributed adaptive formation tracking protocol. One of the main challenges in UAV formation systems is ensuring robust communication and coordination among agents, especially under external disturbances and potential internal collisions. Liu et al. [44] introduced a distributed formation control protocol for heterogeneous UAVs, emphasizing the importance of resilience against deception attacks during event-triggered consensus estimation. This highlights the need for protocols that maintain operational integrity even in the presence of misleading information.

Model Predictive Control is widely used in UAV formations due to its predictive capability and constraint-handling features. Reference [45] focused on disturbance rejection in 3D environments, constructing state estimation and error models using relative information. By integrating backstepping and MPC strategies, the study designed control laws to ensure formation stability and optimized the solution process via ant colony algorithms, demonstrating superior performance over traditional methods. Reference [46] explored distributed MPC algorithms, emphasizing efficient parallel computation through local optimization and one-way neighbor communication. The design balanced energy minimization and control input variations, with simulations validating stability and formation flight effectiveness.

PID Control remains a preferred engineering solution for its simplicity and efficiency, particularly in micro-UAV swarms with limited computational resources. Reference [47] proposed a decentralized strategy based on virtual leader concepts and optimal PID control laws to counteract external disturbances, random fluctuations, and wake vortex coupling. By transforming complex nonlinear problems into independent linear matrix inequality optimizations via T-S fuzzy methods and novel variable transformations, the approach significantly improved design efficiency and tracking performance.

Event-Triggered Control addresses scenarios with environmental uncertainties and limited communication resources. Dou et al. [48] designed an adaptive dynamic programming method for distributed formation control, revealing the potential of event-triggered mechanisms to enhance adaptability and response speed. Reference [49] combined finite-time stability theory with event-triggered formation control, focusing on privacy-preserving methods. The study showed that this approach not only accelerated convergence but also reduced controller update frequency, optimizing communication resources.

Regarding time delays, research on formation tracking control for multi-UAV systems has increasingly focused on complex scenarios where delays coexist with external disturbances. For instance, a fixed-time disturbance observer-based robust tracking controller has been proposed, which utilizes an adaptive compensator to enhance trajectory tracking performance under varying disturbance conditions [50], Recent advances also include the proposal of an adaptive dual-channel event-triggered control scheme specifically for formation tracking and obstacle avoidance. This innovative approach aims to improve the responsiveness of UAVs in complex environments, ensuring that they can navigate effectively while maintaining formation [51]. The study leveraged flight state and desired information errors to design control methods, transforming the problem into asymptotic stability via special matrix decomposition and deriving stability conditions using piecewise continuous Lyapunov functionals.

Reference [52] addressed consensus tracking control for nonlinear multi-agent systems, proposing adaptive event-triggered strategies that integrate asymmetric barrier Lyapunov functions, L-K functionals, and fuzzy logic systems to handle output constraints, delays, and nonlinearities. Bounded estimation methods compensated for faults and errors, with simulations validating semi-global bounded stability and effectiveness.

Current challenges in UAV formation control include computational complexity, real-time performance, and environmental adaptability [53]. As formations scale, communication and control algorithm complexity grow exponentially. Formation control is highly sensitive to time delays, especially in high-speed maneuvers, while dynamic environments (e.g., harsh weather, urban canyons) demand greater stability. These challenges have spurred advancements in edge computing, real-time operating systems, and adaptive control, though comprehensive solutions remain elusive [54].

3. Research Status of Cybersecurity and UAV Systems

The cybersecurity threats to UAV systems are diverse and complex, involving multiple layers such as data, communication, hardware, and software. These threats specifically include communication link threats, threats to the UAV itself, ground control station threats, data security threats, supply chain threats, and human factors and operational security threats. The threats to UAV systems in terms of communication links mainly fall into three categories: Denial-of-Service (DoS) attacks, deception attacks, and eavesdropping attacks. DoS attacks occupy communication resources, preventing legitimate information from being transmitted, such as jamming the communication link between the UAV and the ground station. Eavesdropping attacks passively intercept sensitive data transmitted by UAVs, while deception attacks are considered the most stealthy and destructive, as they inject false data to mislead UAV systems into making erroneous decisions.

UAV Formation Control Under DoS Attacks refers to the system maintaining formation stability and coordination through specific control strategies and algorithms when subjected to malicious attacks. The core of this control mechanism lies in analyzing the impact of attacks on UAV communication and decision-making processes and adopting corresponding defensive measures to ensure the formation can effectively execute predefined tasks and maintain system resilience and reliability in hostile environments.

In the development of UAV formation control under DoS attacks, increasing attention has been paid to the resilience and security of MAS against cyber threats. Various studies have explored different aspects of formation control under DoS attacks, emphasizing the need for robust strategies to preserve operational integrity.

Wang et al. [55] introduced an attack-resilient event-triggered formation control framework for MAS, specifically targeting periodic DoS attacks. Their approach leverages sophisticated Laplacian matrices to enhance system resilience, demonstrating that event-triggered mechanisms can effectively mitigate the impact of such attacks on formation stability. Pan et al. [56] expanded the discussion by investigating multi-channel DoS attacks, where the independence of attacks across channels presents unique challenges. Their findings suggest that existing models, which often assume uniform attack patterns, may fail to fully capture the complexity of real-world scenarios, necessitating more nuanced control strategies. Liu et al. [57] contributed to the discussion by addressing the formation control of cyber-physical systems under DoS attacks and faults. Their distributed control protocol incorporates event-triggered techniques and proactive reconfiguration strategies, showcasing a comprehensive approach to ensuring system resilience against cyber threats. Zheng et al. [58] proposed a distributed secure formation control algorithm for autonomous surface vehicles, focusing on mitigating the impact of DoS attacks through a performance-adjustable event-triggered mechanism. This work highlights the importance of adaptive control strategies in maintaining formation integrity amid network disruptions. Overall, there is a clear trend toward developing sophisticated, adaptive, and resilient control strategies for UAV formations in the face of DoS attacks.

UAV Formation Control Under Deception Attacks refers to the system maintaining decision-making accuracy and mission execution efficiency by implementing specific identification and verification algorithms when encountering false information or misleading instructions. The key to this control strategy lies in assessing the credibility of information sources and monitoring abnormal behavior in real time to ensure UAVs can effectively identify and resist potential spoofing threats, thereby achieving formation security and stability.

Research on deception attacks primarily focuses on two directions: attack modeling and detection methods. In attack modeling, deception attacks are classified into sensor spoofing (e.g., tampering with GPS, visual, or radar perception data) and communication spoofing (e.g., identity impersonation or packet tampering). In detection methods, Kalman filtering, statistical hypothesis testing, and machine learning have emerged as mainstream technical approaches. Wang et al. [59] introduced an adversarial obstacle generation algorithm targeting LiDAR-based 3D object detection systems. Their study highlights the potential for spoofed obstacles to mislead detection algorithms, which is critical for UAVs operating in complex environments. This fundamental understanding of spoofing behavior in sensor systems is essential for developing robust formation control strategies. Study [60] developed an event-triggered formation tracking control method capable of countering cyberattacks, including deception attacks. This approach employs a control protocol that enables UAVs to maintain their formation even under malicious interference. Additionally, study [61] investigated the concept of induced attacks on formation control, where such attacks can covertly manipulate UAV formations, compromising their operational integrity. Recent advances also include research on high-order multi-agent systems under deception attacks, focusing on vulnerabilities in sensor-to-controller communication channels. This research underscores the importance of secure communication protocols in preserving formation integrity against spoofing threats.

Eavesdropping Attacks involve attackers intercepting communication signals between UAVs to obtain sensitive information or disrupt normal operations. The primary objectives of such attacks include information theft and operational interference. Information theft involves acquiring mission instructions, positional data, and other sensitive information from UAV formations. Operational interference enables attackers to manipulate UAV behavior, such as misleading navigation or altering flight paths, by intercepting real-time data. Study [62] explored efforts to detect and prevent eavesdropping attacks on UAVs. Distributed bearing-based formation maneuver control and eavesdropping attack detection have been investigated as potential solutions to mitigate risks posed by malicious actors.

However, existing research has notable limitations: (1) Most methods are designed for single UAV systems and do not account for the security complexities of formation scenarios. (2) Attack detection and defense are often studied as separate problems, lacking integrated solutions. (3) There is a significant gap between theoretical research and practical applications, with many algorithms proving difficult to implement on resource-constrained UAV platforms.

4. UAV Formation Control Under Deception Attacks in Communication

In modern UAV formation control, the impact of communication deception attacks is significant, necessitating in-depth research on defense mechanisms. To effectively address this challenge, it is essential to explore the comprehensive application of multiple defense strategies to enhance the anti-jamming capability and system robustness of UAV formations.

Communication deception attacks refer to malicious acts that disrupt normal communication and cooperative operations of UAV formations by forging or tampering with transmitted information, leading to system decision-making errors or mission failures. Such attacks not only threaten the security of UAV formations but may also severely impact critical infrastructure. Therefore, studying defense mechanisms holds substantial practical significance.

Existing research has proposed various methods to enhance formation control in response to vulnerabilities caused by cyberattacks. Reference [63] focuses on the role of UAVs as communication relays to optimize air-to-ground uplinks. Its

framework combines least-squares estimation for channel approximation and employs a gradient-based relay position optimization method, which is crucial for maintaining effective communication under potential network interference. This foundational study provides a basis for understanding how UAVs mitigate communication challenges. Zhang et al. [64] further advance the field by proposing a power control and clustering-based interference management framework for UAV-assisted networks. Their established non-cooperative game model achieves Nash equilibrium, which is critical for ensuring stable communication when cyberattacks may disrupt normal operations. Huo et al. [65] innovatively propose a pigeon-inspired circular formation control method, leveraging intelligent behavior to maintain formations under limited target information. This approach is particularly suitable for cyberattack scenarios due to its emphasis on adaptive control strategies in response to changing communication environments. Yang et al. [66] specifically investigate the security of Age of Information (AoI) optimization in UAV-assisted networks under channel access attacks (CAA). Through game-theoretic analysis of CAA's impact on network performance, they propose strategies to minimize AoI, highlighting the necessity of constructing attack-resistant robust formation control mechanisms. Suo et al. [67] focus on formation control for fixed-wing UAV swarms in distributed ad-hoc networks. Their proposed route-based formation switching and obstacle avoidance method is of significant value in countering potential interference from cyberattacks and maintaining formation integrity. Fei et al. [68] explore a cooperative search model for multi-UAV systems under limited communication networks. This study emphasizes enhancing collaborative capabilities through flight strategy design, which is particularly critical when communication channels are compromised. Finally, Han et al. [69] propose an intelligent optimization scheme for defending against channel access attacks in UAV-assisted heterogeneous networks. Simulation results demonstrate improvements in AoI, throughput, and latency, underscoring the importance of developing anti-fragile communication strategies.

5. Conclusion

This paper systematically reviews the research status and development trends of UAV formation control under deception attacks. With the rapid advancement of emerging technologies such as artificial intelligence, edge computing, and blockchain, this field is facing unprecedented opportunities and challenges.

5.1. Research Challenges

The core challenges in current research are mainly reflected in four aspects: First, the issue of attack isolation in multi-UAV cooperative environments, which requires precise attack detection and isolation while ensuring formation performance. Second, the trade-off between real-time performance and security, particularly in achieving efficient and secure defense under resource-constrained conditions. Third, the problem of defending against intelligent dynamic attacks, which necessitates countering novel attack methods with adaptive capabilities. Finally, the challenge of heterogeneous system coordination, which involves ensuring secure collaboration among nodes with varying computational capabilities.

5.2. Cutting-Edge Research Directions and Future Prospects

Future research should focus on three key directions: intelligent security defense, adaptive control architectures, and system-level security. In intelligent security defense, deep reinforcement learning-based end-to-end secure control frameworks, blockchain-enabled decentralized secure communication mechanisms, and edge computing-driven distributed secure computing architectures will become important research areas. In adaptive control architectures, the integration of hybrid architectures, the construction of self-organizing networks, and the enhancement of multi-modal perception capabilities will drive the intelligent development of formation control systems. In system-level security, lifecycle security design, cross-domain collaborative defense mechanisms, and the establishment of standardized security evaluation systems will be key research priorities.

With breakthroughs in technologies such as quantum computing and digital twins, UAV formation control will usher in new development opportunities. Secure communication mechanisms based on quantum key distribution, the construction of digital twin models for formation systems, the adoption of bio-inspired swarm intelligence defense mechanisms, and cross-domain collaborative control of multi-UAV systems will become important future research directions. In summary, research on UAV formation control under deception attacks is in a phase of rapid development, requiring joint efforts from academia and industry to advance the field toward greater security, reliability, and intelligence.

Acknowledgments

This work was supported in part by the Guangdong Basic and Applied Basic Research Foundation under Grant 2023A1515010168, in part by the Key Special Foundation for General Universities in Guangdong Province under Grant 2022ZDZX1018, in part by the Maoming Science and Technology Plan Foundation under Grant 2022S043, in part by the National Natural Science Foundation of China Under Grant 62273109, Grant 62333006, Grant 62073144.

References

[1] Grand View Research. Drone Market Size, Share & Trends Analysis Report By Component, By Product, By Technology, By Payload Capacity, By Power Source, By End Use, By Region, And Segment Forecasts, 2025-2030[R]. San Francisco: Grand View Research, Inc., 2024.

[2] Oh K, Park M ,Ahn H .A survey of multi-agent formation control[J].Automatica,2015,53424-440.

[3] Chen W, Liu J, Guo H, et al. Toward robust and intelligent drone swarm: Challenges and future directions[J]. IEEE Network, 2020, 34(4): 278-283.

[4] Liao F, Teo R, Wang J L, et al. Distributed formation and reconfiguration control of VTOL UAVs[J]. IEEE Transactions on Control Systems Technology, 2016, 25(1): 270-277.

[5] Mehran M , Magnus E .Graph Theoretic Methods in Multiagent Networks[M].Princeton University Press:2010-07-01.

[6] Chen Q, Wang T, Jin Y, et al. A UAV formation control method based on sliding-mode control under communication constraints[J]. Drones, 2023, 7(4): 231.

[7] Zhiruo Z, Lei C A O, Xiliang C, et al. UAV intelligent attack strategy generation model based on multi-agent game

reinforcement learning[J]. Systems Engineering & Electronics, 2023, 45(10).

[8] Sarhan A, Qin S. Intelligent Control for Formation Flight of UAVs Based on ANFIS[C]//2017 2nd International Conference on Machinery, Electronics and Control Simulation (MECS 2017). Atlantis Press, 2016: 447-453.

[9] Kamel B, Oussama A. Cooperative Navigation and Autonomous Formation Flight for a Swarm of Unmanned Aerial Vehicle[C]//2021 5th International Conference on Vision, Image and Signal Processing (ICVISP). IEEE, 2021: 212-217.

[10] Pan Z, Zhang C, Xia Y, et al. An improved artificial potential field method for path planning and formation control of the multi-UAV systems[J]. IEEE Transactions on Circuits and Systems II: Express Briefs, 2021, 69(3): 1129-1133.

[11] Zhang P, Wang Z, Zhu Z, et al. Enhanced Multi-UAV Formation Control and Obstacle Avoidance Using IAAPF-SMC[J]. Drones (2504-446X), 2024, 8(9).

[12] Tsao K Y, Girdler T, Vassilakis V G. A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks[J]. Ad Hoc Networks, 2022, 133: 102894.

[13] Check Point Research. 2023 Global Intelligent Systems Security Landscape Report[R]. Tel Aviv: Check Point Software Technologies Ltd., 2023.

[14] DING, DERUI, HAN, QING-LONG, WANG, ZIDONG, et al. A Survey on Model-Based Distributed Control and Filtering for Industrial Cyber-Physical Systems[J]. IEEE transactions on industrial informatics,2019,15(5):2483-2499. DOI:10.1109/ TII. 2019.2905295.

[15] Ao W, Song Y, Wen C. Distributed secure state estimation and control for CPSs under sensor attacks[J]. IEEE transactions on cybernetics, 2018, 50(1): 259-269.

[16] LIU F, XIAO B, CHEN S, et al. A Preferential Recovery Method of Interdependent Networks under Load[J]. Journal of Electronics & Information Technology, 2020, 42(7): 1694-1701.

[17] Feng, Zhi, and Guoqiang Hu. "Distributed secure average consensus for linear multi-agent systems under DoS attacks." 2017 American control conference (ACC). IEEE, 2017.

[18] Yin T, Gu Z, Xie X. Observer-based event-triggered sliding mode control for secure formation tracking of multi-UAV systems[J]. IEEE Transactions on Network Science and Engineering, 2022, 10(2): 887-898.

[19] Xiao J, Feroskhan M. Cyber attack detection and isolation for a quadrotor UAV with modified sliding innovation sequences [J]. IEEE Transactions on Vehicular Technology, 2022, 71(7): 7202-7214.

[20] Miao F, Zhu Q, Pajic M, et al. A hybrid stochastic game for secure control of cyber-physical systems[J]. Automatica, 2018, 93: 55-63.

[21] Zou Y, Xia K, He W. Adaptive fault-tolerant distributed formation control of clustered vertical takeoff and landing UAVs[J]. IEEE Transactions on Aerospace and Electronic Systems, 2021, 58(2): 1069-1082.

[22] The 14th Five-Year Plan for National Economic and Social Development of the People's Republic of China and the Outline of the Long-Term Objectives for 2035[M]. Beijing: People's Publishing House, 2021.

[23] Ministry of Industry and Information Technology. "14th Five-Year Plan" Intelligent Manufacturing Development Plan[Z]. 2022-12-22.

[24] Chinese Society of Aeronautics. China UAV Development Report (2023) [R]. Beijing: Aviation Industry Press, 2023.Li S, Chen Y, Liu P X. Distributed fault detection and dynamic event-triggered consensus for heterogeneous multiagent systems under deception attacks[J]. IEEE Transactions on Circuits and Systems I: Regular Papers, 2023, 70(8): 3294-3304.

[25] Zhu Q, Bushnell L, Başar T. Resilient distributed control of multi-agent cyber-physical systems[C]//Control of Cyber-Physical Systems: Workshop held at Johns Hopkins University, March 2013. Springer International Publishing, 2013: 301-316.

[26] Yuan H, Xia Y, Yang H. Resilient state estimation of cyber-physical system with multichannel transmission under DoS attack[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2020, 51(11): 6926-6937.

[27] Saulnier K, Saldana D, Prorok A, et al. Resilient flocking for mobile robot teams[J]. IEEE Robotics and Automation letters, 2017, 2(2): 1039-1046.

[28] Xu Y, Di L, Chen Y Q. Consensus based formation control of multiple small rotary-wing UAVs[C]//International Design Engineering Technical Conferences and Computers and Information in Engineering Conference. 2011, 54808: 909-916.

[29] Kuriki Y, Namerikawa T. Consensus-based cooperative formation control with collision avoidance for a multi-UAV system[C]//2014 American control conference. IEee, 2014: 2077-2082.

[30] Yuan D, Wang Y. Data driven model-free adaptive control method for quadrotor formation trajectory tracking based on rise and ISMC algorithm[J]. Sensors, 2021, 21(4): 1289.

[31] Ranjan P K, Sinha A, Cao Y, et al. Relational maneuvering of leader-follower unmanned aerial vehicles for flexible formation[J]. IEEE Transactions on Cybernetics, 2024.

[32] Liu R, Qu B, Wei T, et al. Research on UAV formation obstacle avoidance based on consistency control[C]//2023 IEEE 12th Data Driven Control and Learning Systems Conference (DDCLS). IEEE, 2023: 155-160.

[33] Guo J, Qi J, Wang M, et al. Distributed cooperative obstacle avoidance and formation reconfiguration for multiple quadrotors: Theory and experiment[J]. Aerospace Science and Technology, 2023, 136: 108218.

[34] Song S, Zhao T, Zheng J. Research on fault-tolerant algorithm for emergency medical rescue UAV formation[C]//2020 IEEE International Conference on E-health Networking, Application & Services (HEALTHCOM). IEEE, 2021: 1-5.

[35] Zhen R, Jin Y, Wu X, et al. Fault-Tolerant Time-Varying Formation Tracking Control for Unmanned Aerial Vehicle Swarm Systems with Switching Topologies[J]. Mathematical Problems in Engineering, 2021, 2021(1): 5519243.

[36] Hua L, Zhang J, Li D, et al. Fault-tolerant active disturbance rejection control of plant protection of unmanned aerial vehicles based on a spatio-temporal RBF neural network[J]. Applied Sciences, 2021, 11(9): 4084.

[37] Xiang X, Liu C, Su H, et al. On decentralized adaptive full-order sliding mode control of multiple UAVs[J]. ISA transactions, 2017, 71: 196-205.

[38] Fei Y, Sun Y, Shi P. Robust hierarchical formation control of unmanned aerial vehicles via neural-based observers[J]. Drones, 2022, 6(2): 40.

[39] Liu Z, Huang D, Li S, et al. Adaptive robust control of the UAV-USV heterogeneous system with unknown fractional-order dynamics under multiple disturbances[C]//2023 42nd Chinese Control Conference (CCC). IEEE, 2023: 5872-5877.

[40] Yang S, Yu W, Liu Z, et al. A Robust Hybrid Iterative Learning Formation Strategy for Multi-Unmanned Aerial Vehicle Systems with Multi-Operating Modes[J]. Drones, 2024, 8(8): 406.

[41] Raffo G V, de Almeida M M. Nonlinear robust control of a quadrotor UAV for load transportation with swing improvement [C]//2016 American control conference (ACC). IEEE, 2016: 3156-3162.

[42] Hu J, Lanzon A. Cooperative control of innovative tri-rotor drones using robust feedback linearization[C]//2018 UKACC 12th International Conference on Control (CONTROL). IEEE, 2018: 347-352.

[43] Ning J, Huang Y, Liu Z, et al. Adaptive Distributed Heterogeneous Formation Control for UAV-USVs with Input Quantization[J]. Journal of Marine Science and Engineering, 2024, 12(6): 975.

[44] Peng Y, Yan H, Rao K, et al. Distributed model predictive control for unmanned aerial vehicles and vehicle platoon systems: a review[J]. Intelligence & Robotics, 2024, 4(3): 293-317.

[45] Wu Z, Yang F, Zhang B, et al. Distributed Model Predictive Control for Multi-UAV Formation Systems[C]//2024 14th Asian Control Conference (ASCC). IEEE, 2024: 891-896.

[46] Thien R T Y, Kim Y. Decentralized formation flight via PID and integral sliding mode control[J]. Aerospace Science and Technology, 2018, 81: 322-332.

[47] Dou L, Cai S, Zhang X, et al. Event-triggered-based adaptive dynamic programming for distributed formation control of multi-UAV[J]. Journal of the Franklin Institute, 2022, 359(8): 3671-3691.

[48] Yue J, Qin K, Shi M, et al. Event-trigger-based finite-time privacy-preserving formation control for multi-uav system[J]. Drones, 2023, 7(4): 235.

[49] Yue J, Qin K, Shi M, et al. Event-trigger-based finite-time privacy-preserving formation control for multi-uav system[J]. Drones, 2023, 7(4): 235.

[50] Guo Y. Fixed-time disturbance observer based robust tracking control of wheeled mobile robot with multiple disturbances[J]. Measurement and Control, 2023, 56(9-10): 1626-1636.

[51] Liu S, Zhang R, Zhao D, et al. Adaptive dual-channel event-triggered fuzzy control for autonomous underwater vehicles with multiple obstacles environment[J]. IEEE Transactions on Intelligent Transportation Systems, 2024.

[52] Thuyen N A, Thanh P N N, Anh H P H. Distributed event-triggered adaptive finite-time formation control for multiple under-actuated AUVs using command filtered backstepping technique with prescribed performance[J]. European Journal of Control, 2025, 82: 101183.

[53] Ding K, Li Y, Quevedo D E, et al. A multi-channel transmission schedule for remote state estimation under DoS attacks[J]. Automatica, 2017, 78: 194-201.

[54] Wang J, Gao J, Wu P. Attack-resilient event-triggered formation control of multi-agent systems under periodic DoS attacks using complex Laplacian[J]. ISA transactions, 2022, 128: 10-16.

[55] Pan K, Lyu Y, Pan Q. Adaptive formation for multiagent systems subject to denial-of-service attacks[J]. IEEE Transactions on Circuits and Systems I: Regular Papers, 2022, 69(8): 3391-3401.

[56] Liu Y, Dong X, Ren Z, et al. Secure formation control for resilient multi-agent cyber-physical systems under DoS attacks and faults[J]. International Journal of Robust and Nonlinear Control, 2023, 33(6): 3607-3626.

[57] Zheng Y, Zhang L, Huang B, et al. Distributed secure formation control for autonomous surface vessels by performance adjustable event-triggered mechanism[J]. International Journal of Robust and Nonlinear Control, 2023, 33(14): 8490-8507.

[58] Wang J, Li F, Zhang X, et al. Adversarial obstacle generation against lidar-based 3d object detection[J]. IEEE Transactions on Multimedia, 2023, 26: 2686-2699.

[59] Zhang Q, Zhang S, Liu Y, et al. Adaptive terminal sliding mode control for USV-ROVs formation under deceptive attacks[J]. Frontiers in Marine Science, 2024, 11: 1320361.

[60] Li J, Wang L, Xi J, et al. Induced attack on formation control of multiagent systems with prescribed reference trajectories[J]. International Journal of Robust and Nonlinear Control, 2024, 34(12): 8374-8397.

[61] Alzahrani A. Novel approach for intrusion detection attacks on small drones using ConvLSTM model[J]. IEEE Access, 2024.

[62] Wu G, Gao X, Wan K. Mobility control of unmanned aerial vehicle as communication relay to optimize ground-to-air uplinks[J]. Sensors, 2020, 20(8): 2332.

[63] Zhang J, Chuai G, Gao W. Power control and clustering-based interference management for UAV-assisted networks[J]. Sensors, 2020, 20(14): 3864.

[64] Huo M, Duan H, Fan Y. Pigeon-inspired circular formation control for multi-UAV system with limited target information [J]. Guidance, Navigation and Control, 2021, 1(01): 2150004.

[65] Yang Y, Wang W, Xu R, et al. AoI optimization for UAV-aided MEC networks under channel access attacks: A game theoretic viewpoint[C]//ICC 2022-IEEE International Conference on Communications. IEEE, 2022: 1-6.

[66] Suo W, Wang M, Zhang D, et al. Formation control technology of fixed-wing UAV swarm based on distributed ad hoc network[J]. Applied Sciences, 2022, 12(2): 535.

[67] Fei B, Bao W, Zhu X, et al. Autonomous cooperative search model for multi-UAV with limited communication network[J]. IEEE Internet of Things Journal, 2022, 9(19): 19346-19361.

[68] Han Z, Yang Y, Bilal M, et al. Smart optimization solution for channel access attack defense under UAV-aided heterogeneous network[J]. IEEE Internet of Things Journal, 2023, 10(21): 18890-18897.