Proceedings of CONF-FMCE 2025 Symposium: Semantic Communication for Media Compression and Transmission
DOI: 10.54254/2755-2721/2025.GL25197

Collaborative Traffic Monitoring and Management of Autonomous Driving and Unmanned Aerial Vehicle Systems

Liuyi Xu

College of Engineering, Beijing Forestry University, Beijing, China
13761899576@163.com

Abstract. With the rapid advancement of Intelligent Transportation Systems (ITS), the collaboration between autonomous driving and unmanned aerial vehicle (UAV) technologies has attracted significant attention in traffic monitoring and management. Traditional methods like ground cameras and sensors, while providing specific data, face limitations in complex road conditions, dynamic environments, and emergency responses. This article reviews the current applications of autonomous driving and UAV systems in traffic monitoring, analyzing their collaborative potential in data collection, transmission, processing, and decision-making. A 5G/6G and edge computing-based collaborative monitoring framework is proposed, enabling UAVs as mobile sensing nodes to enhance real-time traffic data acquisition. The integration mechanisms, advantages, and challenges of drones and autonomous vehicles in intelligent traffic management are also examined. Current research indicates that UAV-autonomous driving cooperation improves traffic monitoring coverage and accuracy, benefiting accident warning, dynamic routing, and intelligent signal control. Future advances in communication and AI will deepen this integration, fostering more efficient and safer intelligent transportation systems.

Keywords: Autonomous Driving, Unmanned Aerial Vehicles (UAVs), Intelligent Traffic Management

1. Introduction

With the rapid development of autonomous driving technology and unmanned drone system, intelligent transportation systems are gradually moving from theoretical concepts to practical applications. Autonomous vehicles achieve environmental perception and decision control through multiple sensors, while drones demonstrate unique advantages in traffic monitoring and emergency response due to their flexibility and wide coverage capabilities [1]. The collaboration enhances traffic management's real-time accuracy and reliability by using drones for global road data collection, optimizing route planning via vehicle local perception, and jointly addressing incidents like traffic accidents [2]. However, this collaborative work still faces several challenges: the data fusion of multi-source heterogeneous sensors relies on high-precision calibration, and traditional calibration methods are susceptible to insufficient data frames or noise interference in dynamic scenes [3]; the open architecture of vehicle networks makes them vulnerable to network attacks, and interpretable artificial intelligence (XAI) needs to be combined to enhance the transparency and robustness of intrusion detection: the real-time and reliability of cooperative communication need to rely on 5G/6G network and edge computing technology to meet the requirements of high concurrent data transmission and low latency [2].

This article aims to systematically review the key technologies of collaborative traffic monitoring and management between autonomous driving and unmanned aerial vehicles, focusing on analyzing the progress of network security protection and XAI applications, by integrating cutting-edge research results, exploring the technological bottlenecks and future directions of collaborative systems, and providing theoretical support for the practice of intelligent transportation.

2. Technical background and core concepts

2.1. Fundamentals of autonomous driving technology

The core of autonomous driving technology is multi-layer environmental awareness and decision-making control. The perception layer obtains high-precision 3D point cloud data through Light Laser Detection and Ranging (LiDAR), combined with texture information captured by cameras, to comprehensively analyse the scene [3]. For example, LiDAR measures the distance to a target by emitting a laser beam. The decision-making layer relies on V2X communication technology to achieve information exchange between vehicles and infrastructure (V2I), vehicles and vehicles (V2V), supporting dynamic path planning and collaborative obstacle avoidance [1]. Conventional in-vehicle network protocols like CAN bus lack integrated encryption, rendering them vulnerable to physical layer intrusions and message injection attacks at the data link layer [1].

2.2. The character of UAV in traffic management

The application of UAVs in traffic management has become increasingly widespread, particularly in developing Intelligent Transportation Systems (ITS), where they play a critical role. Traditional traffic monitoring systems mainly rely on fixed ground-based cameras or traffic sensors. While these devices cover key traffic nodes, they often struggle to cope with complex traffic environments and unexpected incidents. The introduction of UAVs offers a more flexible and efficient solution for traffic monitoring and management.

As aerial mobile nodes, UAVs undertake multiple tasks in traffic management:

First, UAVs can collect real-time, global traffic data, compensating for the blind spots of traditional fixed monitoring equipment. Leveraging aerial imagery and LiDAR technology, they produce detailed traffic heatmaps that facilitate real-time road condition monitoring and optimize local vehicular route planning [2]. This image data supports traffic control personnel in performing flow prediction and emergency response. In densely populated urban environments, UAV-enabled traffic surveillance facilitates real-time optimization of transportation networks, thereby mitigating congestion and enhancing traffic flow efficiency.

Second, UAVs have emergency response capabilities. In traffic accidents or other emergencies, they can rapidly arrive at the scene for on-site assessment and provide support. UAVs can transport medical devices, first-aid kits, and critical supplies, enabling rapid deployment to accident locations and providing essential support for emergency response operations [2].

Lastly, building a vehicle-to-UAV (V2U) relay network extends the coverage of V2X communication. This enables vehicles to transmit information without being restricted by ground infrastructure, effectively mitigating signal attenuation caused by the “urban canyon effect” [2].

DOI: 10.54254/2755-2721/2025.GL25197

2.3. Communication framework of cooperative systems

The communication framework of cooperative systems is the technical foundation for efficient collaboration between autonomous vehicles and UAVs. Its core objective is to ensure low-latency, high-reliability, and high-bandwidth data transmission among multiple nodes. Presently, this architecture predominantly integrates wireless communication technologies including 5G/6G cellular networks, Dedicated Short-Range Communications (DSRC), and Cellular Vehicle-to-Everything (C-V2X) protocols [3].

On this basis, edge computing and Multi-access Edge Computing (MEC) architectures are introduced to enable localized processing of sensing, decision-making, and response functions. This reduces the load on cloud systems and lowers communication latency. A typical cooperative communication system consists of three key components:

Aerial platform (UAVs): Serving as high-altitude mobile sensing nodes, UAVs must maintain stable links to transmit video, LiDAR, and other data in real time to ground systems.

Ground autonomous vehicles: These vehicles exchange position, speed, and environmental information with other traffic participants through V2V (Vehicle-to-Vehicle), V2I (Vehicle-to-Infrastructure), and V2U (Vehicle-to-UAV) communication.

Infrastructure nodes (e.g., RSUs and edge servers): These provide computational resources, perform road condition fusion analysis, and issue security strategies [1].

Millimeter-wave communication and massive MIMO have expanded system capacity and coverage. To improve link stability, multi-hop communication and UAV-based self-organizing networks enhance robustness. AI-driven dynamic resource allocation optimizes bandwidth in multi-user access, prioritizing critical tasks like emergency obstacle avoidance.

2.4. Network security and explainable artificial intelligence (XAI)

The openness of UAV–vehicle cooperative systems exposes them to a broad attack surface, including data link layer DoS attacks, application-layer malware injection, and spoofing attacks targeting sensor calibration parameters [1]. Therefore, a range of targeted technologies is needed to enhance system defenses:

Encryption and authentication: Strengthening communication security through additional encryption and authentication processes. Lightweight Physical Unclonable Functions (PUFs) secure UAV communication links, while CAN-FD protocols enhance message authentication within vehicle networks [1].

XAI-driven intrusion detection: Techniques such as SHAP (Shapley Additive Explanations) and LIME (Local Interpretable Model-agnostic Explanations) are used to interpret the decision logic of detection models, thereby improving detection transparency. For instance, entropy-based anomaly detection methods analyze CAN bus traffic patterns to identify DoS attack signatures, achieving detection accuracies as high as 98% [1].

These approaches aim to increase robustness against known threats and offer interpretable models that allow operators and system designers to understand, trust, and verify security decisions made by AI-based systems. This is particularly critical in dynamic, safety-critical environments such as intelligent transportation networks.

DOI: 10.54254/2755-2721/2025.GL25197

3. The key technology of the communication framework

3.1. Data fusion and real-time processing

Cooperative monitoring between autonomous vehicles and UAV systems relies on the fusion and real-time analysis of heterogeneous data from multiple sources. UAVs collect global traffic status data using high-resolution cameras, LiDAR, and GPS sensors, while autonomous vehicles provide localized perception data.

Applying object detection and tracking algorithms such as YOLOv4 and DeepSORT, combined with Kalman filtering and particle filtering (e.g., Interacting Multiple Model Particle Filter, IMM-PF) can achieve high-precision target localization in dynamic traffic environments. Moreover, real-time data collected by large-scale UAV swarms has demonstrated the capability of multimodal traffic parameter analysis, such as lane change frequency and travel time [4].

However, challenges remain in data synchronization and timestamp alignment. These are critical for ensuring consistency across different data sources. To meet low-latency requirements, edge computing is employed to optimize computational efficiency and reduce reliance on centralized processing.

3.2. Network security and privacy protection

In the cooperative architecture between autonomous vehicles and UAV systems, network security and privacy protection are fundamental to stable system operation and establishing user trust. Considering these systems rely extensively on high-frequency V2X communication and real-time data exchange, both vehicular trajectory data and sensor inputs gathered by UAVs are vulnerable to cyber threats.

Common attack types include data injection, denial-of-service (DoS) attacks, and GPS spoofing. These threats not only disrupt system services but may also directly endanger the safety of traffic participants. To enhance security, the system described in this paper adopts a multi-layered protection strategy:

At the communication link level, end-to-end encryption and lightweight authentication mechanisms are introduced. For example, Physical Unclonable Functions (PUFs) combined with digital signature schemes enhance the tamper resistance of communication. Access control strategies and blockchain technologies—such as the UTM-Chain structure—are applied at the application level to ensure data exchange between UAVs and vehicles is traceable and non-repudiable.

For privacy protection, differential privacy algorithms and federated learning frameworks are employed to desensitize personal information in UAV imagery, achieving the goal of "data usability without visible privacy." [5] Future privacy protection must align with legal frameworks and establish data governance models for city-scale intelligent transportation systems, ensuring technology respects citizen rights and ethics.

3.3. Intrusion detection and anomaly response

Given that UAVs and autonomous vehicles are often interconnected via wireless links, their distributed and highly dynamic nature creates a more complex attack surface than traditional networks. Therefore, establishing efficient intrusion detection and anomaly response mechanisms is essential to ensure the stability of cooperative systems.

DOI: 10.54254/2755-2721/2025.GL25197

Studies show that traditional rule-based intrusion detection methods—for example, collision warning algorithms based on motion vectors using Optical Flow and Blob Detection—are limited in handling novel attack patterns, often resulting in missed or false alarms [6]. This paper addresses intrusion detection by employing Explainable AI (XAI) models. Techniques like LIME and SHAP enable visualization and interpretation of deep learning decisions, improving detection of abnormal traffic and behaviors.

For instance, by combining CAN bus entropy analysis with graph neural networks (GNNs), it becomes possible to identify abnormal packet frequency and deviations in node behavior patterns, thereby precisely locating potential sources of attack. In terms of anomaly response, this paper proposes a collaborative response mechanism based on V2X communication. Locally detected anomalies are rapidly broadcast to neighboring vehicles and UAVs, enabling multi-agent collision avoidance, emergency deceleration, and route reconfiguration [7].

Edge computing nodes perform model inference and alerting to reduce latency and enhance real-world deployment. Future research should focus on model compression and distillation for lightweight hardware, enabling broad deployment on vehicle and UAV terminals. Additionally, integrating threat modeling and red-teaming will continuously improve cybersecurity strategies.

3.4. Cooperative decision-making and resource scheduling

In a cooperative traffic system composed of UAVs and autonomous vehicles, efficient decision-making and resource scheduling are key to maintaining operational stability and quality of service. For example, low-altitude traffic management schemes based on Aerial Corridors support coordinated multi-UAV formations, with collaborative path planning algorithms designed to minimize monitoring blind spots [8].

Given the highly dynamic and spatially uneven nature of traffic scenarios, the system must dynamically adjust task assignments, computational loads, and communication resources based on real-time perception data. UAV swarms can be strategically deployed across high-traffic road segments, accident hotspots, or traffic signal junctions utilizing formation flight patterns or regional segmentation techniques.

This enables differentiated monitoring and adaptive task prioritization.

To improve system intelligence, reinforcement learning has been increasingly applied in multi-agent decision-making. For example, Deep Q-Network (DQN)-based scheduling algorithms can dynamically optimize UAV trajectories, sensor resolutions, and operational altitudes to enhance sensing coverage while adhering to energy limitations. Meanwhile, autonomous vehicles can adjust their driving strategies based on global traffic insights provided by UAVs, enabling traffic dispersion, route reconfiguration, and coordinated obstacle avoidance.

The system can also dynamically adjust task assignment weights based on traffic density and risk predictions to ensure that high-priority areas receive monitoring first. IIn resource allocation, reinforcement learning can optimize UAV altitude and camera resolution to achieve an optimal trade-off between energy efficiency and surveillance accuracy.

However, challenges remain in the standardization of communication protocols among heterogeneous devices—such as compatibility between IEEE 802.11p and 5G NR. At the protocol layer, inter-device coordination still depends on bridging communication standards, and the interoperability between 5G NR and IEEE 802.11p remains a technical bottleneck. Future city-scale traffic cooperative systems will integrate AI scheduling algorithms, adaptive communication, and cloud-edge collaboration to enhance resource allocation and coordinated task execution.

DOI: 10.54254/2755-2721/2025.GL25197

4. Challenges and open issues

4.1. Technical challenges

Existing models are constrained by limitations in real-time performance and computational resources. The computational capacity of onboard systems in UAVs and autonomous vehicles is constrained, hindering the real-time execution of complex algorithms. Consequently, strategies like model compression and quantization are essential. Additionally, robustness challenges in multi-source data fusion can cause temporal and spatial misalignments across sensors, potentially leading to erroneous decision-making. Adaptive calibration algorithms are needed to address these synchronization issues [9]. UAV systems also require enhanced adaptability to complex environments. Adverse weather conditions and the "urban canyon effect" may affect UAV navigation and communication stability. To cope with these challenges, redundant multi-modal sensor designs should be considered to improve fault tolerance [2].

4.2. Security and ethical issues

Collaborative monitoring systems involving multiple UAVs and autonomous vehicles pose significant risks of privacy leakage. Wide-area surveillance by UAVs may infringe on individual privacy, necessitating the establishment of ethical standards and legal boundaries for data collection. Conflicts in airspace management pose significant operational challenges during deployment. The unresolved integration of low-altitude UAVs alongside manned aircraft underscores the critical need for standardized global airspace classification frameworks. Additionally, the ambiguity surrounding liability allocation between autonomous vehicles and UAVs within cooperative systems raises potential legal risks. Establishing clear liability distribution protocols in these integrated systems is an urgent priority.

5. Conclusion

This review examines autonomous driving and UAV collaboration in traffic management, proposing an intelligent framework using advanced communication and edge computing. UAVs enhance traffic sensing by overcoming coverage and response limitations. UAV and autonomous vehicle collaboration improves traffic data timeliness and environmental perception for smarter decisions. Low-altitude traffic management (U1/U2) nears commercialization (TRL 6–7), but advanced services (U3/U4) are limited by hardware and algorithm generalizability. 5G/6G and edge computing improve data processing and real-time response for applications like accident warning and route adjustment. Large-scale deployment faces standardization, regulation, security, and privacy challenges. Future research should focus on data fusion, algorithm robustness, and urban road testing to integrate autonomous vehicles and UAVs into smart city transportation systems.

References

[1] Guan, T., Han, Y., Kang, N., Tang, N., Chen, X., & Wang, S. (2022). An overview of vehicular cybersecurity for intelligent connected vehicles. Sustainability, 14(9), 5211

[2] Nwakanma, C. I., Ahakonye, L. A. C., Njoku, J. N., Odirichukwu, J. C., Okolie, S. A., Uzondu, C., ... & Kim, D. S. (2023). Explainable artificial intelligence (xai) for intrusion detection and mitigation in intelligent connected vehicles: A review.Applied Sciences, 13(3), 1252.

[3] Guo, Z., & Xiao, Z. (2021). Research on online calibration of lidar and camera for intelligent connected vehicles based on depth-edge matching.Nonlinear Engineering, 10(1), 469-476

DOI: 10.54254/2755-2721/2025.GL25197

[4] Dibaei, M., Zheng, X., Jiang, K., Abbas, R., Liu, S., Zhang, Y., ... & Yu, S. (2020). Attacks and defences on intelligent connected vehicles: A survey.Digital Communications and Networks, 6(4), 399-421.
[5] Kopardekar, P., Rios, J., Prevot, T., Johnson, M., Jung, J., & Robinson, J. E. (2016, June). Unmanned aircraft system traffic management (UTM) concept of operations. InAIAA AVIATION Forum and Exposition (No. ARC-E-DAA-TN32838).
[6] Chu, W., Wuniri, Q., Du, X., Xiong, Q., Huang, T., & Li, K. (2021). Cloud control system architectures, technologies and applications on intelligent and connected vehicles: a review. Chinese Journal of Mechanical Engineering, 34(1), 139.
[7] Wang, B., Han, Y., Wang, S., Tian, D., Cai, M., Liu, M., & Wang, L. (2022). A review of intelligent connected vehicle cooperative driving development. Mathematics, 10(19), 3635
[8] Shrestha, R., Oh, I., & Kim, S. (2021). A survey on operation concept, advancements, and challenging issues of urban air traffic management.Frontiers in Future Transportation, 2, 626935.
[9] Lappas, V., Zoumponos, G., Kostopoulos, V., Lee, H. I., Shin, H. S., Tsourdos, A., ... & Trifas, A. (2022). EuroDRONE, a European unmanned traffic management testbed for U-space. Drones, 6(2), 53