ISSN:2790-1688 Volume-15-(2025)

Edge Computing-Assisted AI for Wireless Communication: Cross-Scenario Integration, Security, and Resource Optimization

Yixuan Qian

Nanjing University of Posts and Telecommunications, Nanjing, China

15306267345@163.com

Abstract. With the rapid deployment of 5G and the appearance of 6G, wireless communication is transitioning from connection-oriented to intelligent service-oriented networks. Edge computing and artificial intelligence (AI) have been generally recognised as critical enablers for solving latency, scalability, and security barriers, but existing research is fragmented and scenario-specific. UAV networks, self-driving cars, and smart cities are the three sample domains in which this study provides a comprehensive review and comparative analysis of edge-AI integration. The results show that although AI-driven solutions increase adaptability and decision-making accuracy, edge computing enhances real-time responsiveness, resource efficiency, and data security. Large-scale implementation is hampered by methodological and practical limitations, such as a dependence on simulation studies, a lack of cross-scenario collaboration, and a lack of uniform standards, as the review finds. Furthermore, because it is a literature-based study, this research is limited in its coverage of new application areas outside of the three main scenarios and does not offer empirical confirmation. Therefore, future studies should concentrate on robust security frameworks, adaptive scheduling techniques, lightweight cross-scenario AI models, and standardised assessment systems that are backed by practical testing. These directions will be crucial for realizing secure, scalable, and intelligent wireless communication in the 6G era.

Keywords: Edge Computing, AI-Enabled Wireless Communication, Cross-Scenario Integration, Resource Optimization.

1. Introduction

With the large-scale deployment of 5G advanced technology and the accelerated development of 6G networks, wireless communication transforms from "connection-oriented" to "intelligent service-oriented" [1]. The redundant data generated by massive IOT devices (such as sensors and vehicle terminals) continues to occupy the bandwidth of the core network, increasing the operation cost and posing the risk of privacy disclosure in uploading sensitive data. In this context, edge computing deploys computing power and storage resources at the network's edge close to the data generation source by virtue of the "localization processing" feature, which can reduce the delay to the millisecond level and reduce redundant data transmission. Mobile Edge Computing（MEC） brings computational capabilities closer to the network edge, reducing latency and bandwidth consumption by processing data locally[2]. Wireless communication systems continue to develop, with the development of artificial intelligence algorithms [3]. AI technology (such as deep learning and reinforcement learning) can optimize the communication system's channel estimation, spectrum allocation, and interference suppression performance dynamically. The deep integration of the two has become the key path to breaking through the bottleneck of wireless communication scenarios.

Although the application of edge computing and AI in wireless communication has progressed, the existing research still has significant limitations. Current research mainly focuses on single-domain optimization, such as UAV task offloading, autonomous driving task allocation, and IoT resource management, but lacks cross-scenario coordination, leading to resource conflicts. Meanwhile, distributed edge nodes face serious security risks and fragmented protection schemes, while inconsistent access protocols and the absence of a unified evaluation system hinder large-scale deployment. These issues highlight the urgent need for research on cross-scenario integration, security protection, and resource optimization in edge computing-assisted AI wireless

communication. Motivated by these gaps, this paper conducts a systematic review and comparative analysis of representative scenarios such as UAVs, autonomous driving, and smart cities, aiming to build a unified framework for edge-AI integration. The purpose is to identify core challenges, clarify technical opportunities, and propose research directions that can support secure, scalable, and intelligent wireless communication for next-generation networks.

2. Related Work

2.1 Edge Computing and UAV Fusion

The essence of the application of edge computing in the field of UAV is to solve the core contradiction between "lightweight security requirements of UAV" and "high computing power consumption of autonomous tasks" by combining the computing power of edge nodes (such as ground cloud nodes and adjacent edge servers) with the mobile sensing ability of UAV. Its core logic is: due to the limitations of size and weight of UAV, the onboard computing power and battery capacity are difficult to support autonomous tasks such as real-time computer vision (such as target detection and depth estimation), path planning, and cluster collaboration.

Several approaches have been proposed. Some studies optimize offloading strategies for visual navigation, combining 5G edge computation with lightweight onboard sensing [4]. Others focus on UAV clusters, introducing federated learning and reinforcement learning to improve task allocation and balance resource consumption across dynamic networks [5]. In addition, the fusion of edge AI with UAV systems has been investigated through federated learning, model compression, and multi-access edge computing, which collectively enhance efficiency and adaptability in navigation and collaboration tasks [6]. More recent work has combined lightweight object detection models (e.g., YOLO) with embedded edge devices to enable real-time UAV detection in security-sensitive environments [7].

Existing studies have significantly advanced UAV autonomy by enabling low-cost lightweight drones to perform target detection and obstacle avoidance through edge offloading, thereby reducing reliance on expensive equipment and lowering the application threshold. They also demonstrate flexible scene adaptability, supporting both single-UAV patrols and cluster collaboration, while lightweight designs help balance safety and regulatory compliance. However, limitations remain: lightweight hardware suffers from thermal and performance constraints, heavy reliance on 5G/LTE makes systems vulnerable to latency in remote areas, and current solutions lack robustness in extreme environments or complex scenarios. Moreover, multi-edge collaboration and cross-scenario task migration are still underexplored, hindering the stable operation of large-scale UAV clusters. In summary, while edge-enabled UAV systems demonstrate strong potential for autonomy and cost reduction, their scalability is limited, highlighting the need for more robust, collaborative, and adaptive solutions that will be discussed in the following section.

2.2 Edge Computing-enabled Automatic Driving

Autonomous driving requires powerful AI capabilities for perception, decision-making, and control, yet the limited computing power and energy of onboard devices often hinder real-time performance. To overcome this bottleneck, researchers have proposed edge offloading frameworks in which roadside units and mobile edge servers handle intensive tasks such as sensor fusion, path planning, and VNF deployment [8] [9]. Optimization models and deep reinforcement learning algorithms have been applied to improve resource allocation and ensure continuity of driving functions, while platforms such as the Edge Driving Robot Platform (EDRP) and Local Dynamic Map (LDMP) enable cooperative perception and information sharing among vehicles [10]. For indoor autonomous vehicle scenarios, lightweight hardware combined with LiDAR sensors and neural networks has been used to achieve accurate navigation with balanced energy consumption [11]. These advances improve cost efficiency by reducing reliance on high-end hardware, enhance adaptability across outdoor fleets, indoor AGVs, and multi-robot systems, and in some cases align with

communication and security standards, increasing commercialization potential. Nevertheless, the solutions remain highly dependent on 5G/LTE networks, making them vulnerable in remote or interference-heavy environments. Moreover, existing studies often focus on simplified or static scenarios, with limited validation under extreme weather or highly dynamic traffic conditions, while multi-edge collaboration and high-precision scheduling are still insufficiently explored.

2.3 Edge Computing-enabled Smart City

The essence of the application of edge computing in smart cities is to solve the core contradiction between "massive real-time data processing" and "centralized cloud high latency" by deploying computing power at edge nodes close to the data source. For smart cities, edge computing can make tasks such as traffic control and IOT device monitoring eliminate the dependence on the cloud and realize localized real-time response; For automatic driving, it can reduce the transmission delay of vehicle road cooperation data and ensure the millisecond decision-making requirements. In short, edge computing, through the collaboration of "distributed computing power+AI+wireless communication", has become the underlying technical pillar supporting the efficient operation of smart cities and the safe landing of autonomous driving.

Representative research focuses on "edge computing to break through the bottleneck of smart city operation", but forms differentiated solutions for different sub-scenarios. Representative research explores a multi-level collaborative architecture that integrates cloud, fog, and edge. There are also studies that apply technologies such as federated learning, blockchain, and virtualization to balance efficiency, security, and scalability [12]. In response to the contradiction between network security and performance of heterogeneous IoT in smart cities, the IB-SEC framework was designed. The African buffalo optimization algorithm is used to select the optimal nodes and paths, and distributed hash encryption and secure edge computing are combined to balance energy consumption, latency, and data protection [13]. Additionally,, build a "IOT edge cloud" three-tier architecture around the IOT driven smart city resource allocation, and use the auction mechanism to dynamically match tasks and edge nodes (including UAV edge nodes) to solve the problem of heterogeneous equipment collaboration and delay energy consumption balance[14]. Also, focusing on UAV assisted innovative city traffic management, a multi-objective simulated annealing (Mosa) algorithm is proposed to optimize the task allocation of edge nodes, taking into account the number of active nodes, energy consumption and task execution efficiency. At the same time, UAV data collection, Yolo detection, and enhanced learning traffic control are integrated to form an end-to-end process[15].

In terms of benefits, current research shows that edge computing significantly improves the feasibility of smart city applications by replacing cloud transmission with localised processing, lowering latency and energy consumption, and integrating AI, wireless communication, and UAV technologies into a comprehensive deployment framework. These approaches also show strong adaptability across domains such as big data, heterogeneous IoT, traffic management, and resource allocation, while introducing encryption and authentication mechanisms to mitigate privacy and security risks. However, most solutions are still evaluated in simulation, have the possibility for single-point failure, and lack standardised interfaces and protocols for cross-project reuse. Furthermore, trade-offs between performance, energy efficiency, and security remain unsolved, providing obstacles to large-scale and dependable smart city deployment.

3. Open Challenges and Future Research Directions

3.1 Technical challenges and research directions

In the cross-scenario application of edge AI, the core technical contradiction lies in balancing resource constraints, algorithm adaptation, and data reliability. Key challenges include: (1) a mismatch between the high computing demands of autonomous driving tasks and the limited capacity of IoT devices, which lightweight techniques like pruning and quantization cannot fully resolve [16]; (2) significant overhead in switching between different algorithms, such as real-time scheduling for

autonomous driving and batch detection for IoT, which reduces overall efficiency; and (3) unreliable data inputs caused by channel switching in fast-moving vehicles and environmental interference in IoT devices, leading to unstable AI decisions and service quality.

Future research should focus on three directions: developing lightweight cross-scenario AI models through techniques like knowledge distillation; designing adaptive scheduling mechanisms that dynamically adjust algorithms according to scenario needs; and enhancing robustness by incorporating channel variations and device mobility into model inputs to improve stability across dynamic environments.

3.2 Security and privacy challenges and research directions

The distributed deployment of edge nodes and cross-scene data sharing aggravates the risk superposition of "node security - Data Privacy - artificial intelligence robustness". At the challenge level, one is that edge nodes are vulnerable to attack: distributed edge nodes are primarily deployed in uncontrolled environments (such as outdoor roadside units and industrial workshop gateways), facing risks such as physical tampering and side channel attacks (such as cracking encryption keys through power analysis). There is a lack of unified security protection standards, and the protection schemes of different manufacturers are fragmented, further increasing the possibility of node intrusion. Second, data privacy risk superposition: sensitive control data of automatic driving (such as vehicle braking instructions) and user data of the Internet of Things (such as medical sensor data) are often shared, stored, or processed at edge nodes. Once a security vulnerability occurs at a node, the privacy risk of the two types of data rises synchronously, threatening the safety of automatic driving operation and the privacy of Internet of Things users. Third, AI confrontational threats are prominent: the explosive growth in Mobile Edge Computing paves the way for a new network to spawn fake news[17]. Attackers can forge automatic driving or Internet of Things data (such as generating false traffic signal instructions and tampering with industrial temperature data), and avoid the detection mechanism of edge AI by resisting samples, resulting in AI being unable to accurately identify security threats and aggravating the security risks of the two scenarios.

Future research should focus on three directions: (1) building a unified edge node security framework with lightweight encryption and hardware-level protection, supported by industry-wide certification standards; (2) advancing privacy-preserving computing through federated learning and differential privacy to safeguard IoT and autonomous driving data while maintaining AI accuracy; and (3) enhancing AI robustness by training with diverse adversarial samples to improve detection of forged data and resist attacks.

3.3 standardization challenges and research directions

The lag of standardization is the key obstacle restricting the large-scale application of edge AI across scenes. The core issues focus on "interface compatibility" and "evaluation system". The specific challenges and improvement paths are as follows. From the perspective of challenges, one is that the cross scene interface is not unified: the deployment protocol of the virtual network function of autonomous driving is lack of compatibility with the device access protocols of the Internet of things (such as COAP and mqtt), and the difference in interface standards makes it difficult for the two types of devices to efficiently access the same edge platform, unable to achieve smooth cross scene data interaction and resource collaboration, which restricts the large-scale application of edge AI. Second, there is a lack of a performance evaluation system: there is currently a lack of multi-dimensional evaluation indicators covering "delay resource security". For example, the delay threshold, resource utilization, and attack detection rate of edge AI security decision-making have not been clearly defined, and the cross-scene comprehensive performance of edge AI cannot be comprehensively measured, which is not conducive to the clarification of technology optimization direction, but also hinders the construction of industry unified standards. Future standardization research needs to focus on two aspects: first, unify the edge AI wireless communication interface - industry organizations (such as 3GPP and IEEE) formulate standards and specifications, clarify the

edge interaction format between the autonomous virtual network function and the IOT security module (including data encryption fields, detection result feedback methods), and the allocation rules of wireless channel resources, to realize the seamless access of two types of devices; Second, establish a multi-dimensional performance evaluation system -- build a joint evaluation index of "delay resource utilization attack detection rate", and set a quantitative benchmark for different scenarios (e.g., the delay in the automatic driving scenario should be $\leqslant$ 10 milliseconds, and the delay in the Internet of things scenario should be $\leqslant$ 50 milliseconds), to provide a basis for the unification of technical iteration and industry standards.

4. Conclusion

In conclusion, this paper systematically reviewed the integration of edge computing and artificial intelligence in wireless communication, focusing on three representative scenarios: UAV networks, autonomous driving, and smart cities. The review highlights that edge-assisted AI has the potential to overcome the latency, scalability, and security bottlenecks of cloud-based systems. Across different domains, edge computing enables UAVs to achieve lightweight autonomy, supports real-time decision-making in autonomous driving, and improves responsiveness and data security in smart city applications. These findings confirm the crucial role of edge-AI convergence in supporting the transition toward secure, scalable, and intelligent next-generation communication systems.

However, this study also has methodological limitations. As a literature-based review, it synthesizes existing findings but does not provide empirical validation or experimental benchmarking, which may limit the generalizability of the conclusions. Future research should therefore move beyond conceptual synthesis toward experimental verification and cross-domain case studies.

References

[1] Z. Qin, L. Liang, Z. Wang, et al., "AI empowered wireless communications: From bits to semantics," Proc. IEEE, vol. 112, no. 7, pp. 621–652, Jul. 2024.

[2] D. H. Nam, "A comparative study of mobile cloud computing, mobile edge computing, and mobile edge cloud computing," in Proc. 2023 Congr. Comput. Sci., Comput. Eng., Appl. Comput. (CSCE), Las Vegas, NV, USA, Jul. 24–27, 2023.

[3] M. S. Hossain, M. R. Islam, A. Alkhayyat, et al., "Blockchain-enabled secure data sharing framework for IoT-based healthcare systems using edge computing," IEEE Internet Things J., vol. 10, no. 16, pp. 14213–14228, Aug. 2022.

[4] S. Hayat, R. Jung, H. Hellwagner, et al., "Edge computing in 5G for drone navigation: What to offload?" IEEE Robot. Autom. Lett., vol. 6, no. 2, pp. 2571–2578, Apr. 2021.

[5] D. Rahbari, M. M. Alam, Y. Le Moullec, et al., "Fast and fair computation offloading management in a swarm of drones using a rating-based federated learning approach," IEEE Access, vol. 9, pp. 113832–113849, Aug. 2021.

[6] P. McEnroe, S. Wang, and M. Liyanage, "A survey on the convergence of edge computing and AI for UAVs: Opportunities and challenges," IEEE Internet Things J., vol. 9, no. 17, pp. 15435–15459, Sep. 2022.

[7] R. H. and A. R., "Edge computing-driven real-time drone detection using YOLOv9 and NVIDIA Jetson Nano," Drones, vol. 8, no. 11, p. 680, Nov. 2024.

[8] H. Ibn-Khedher, M. Laroui, H. Moungla, et al., "Next-generation edge computing assisted autonomous driving based artificial intelligence algorithms," IEEE Access, vol. 10, pp. 53987–54001, May 2022.

[9] H. Ibn-Khedher, M. Laroui, M. B. Mabrouk, et al., "Edge computing assisted autonomous driving using artificial intelligence," in Proc. 2021 Int. Wireless Commun. Mob. Comput. (IWCMC), Harbin City, China, Jun. 28–Jul. 2, 2021.

[10] J. Moon, D. Hong, J. Kim, et al., "Enhancing autonomous driving robot systems with edge computing and LDM platforms," Electronics, vol. 13, no. 14, p. 2740, Jul. 2024.

[11] Y. Kwon, W. Kim, and I. Jung, "Neural network models for driving control of indoor autonomous vehicles in mobile edge computing," Sensors, vol. 23, no. 5, p. 2575, Feb. 2023.

[12] M. Trigka and E. Dritsas, "Edge and cloud computing in smart cities," Future Internet, vol. 17, no. 3, p. 118, Mar. 2025.

[13] R. R. Irshad, S. Hussain, I. Hussain, et al., "An intelligent buffalo-based secure edge-enabled computing platform for heterogeneous IoT network in smart cities," IEEE Access, vol. 11, pp. 69282–69294, Jun. 2023.

[14] O. A. Mahmood, A. R. Abdellah, A. Muthanna, et al., "Distributed edge computing for resource allocation in smart cities based on the IoT," Information, vol. 13, no. 7, p. 328, Jul. 2022.

[15] M. A. Khan, F. Ali, M. Aslam, et al., "Edge computing-enabled UAV-assisted data collection and processing for smart agriculture: A survey," IEEE Access, vol. 12, pp. 85244–85268, Jul. 2024.

[16] L. Xia, D. Guo, Y. Wang, et al., "Optimal load scheduling based on mobile edge computing technology in 5G dense networking," in Proc. 2022 3rd Asia Conf. Comput. Commun. (ACCC), Shanghai, China, Dec. 16–18, 2022.

[17] S. Alzubi and F. M. Awaysheh, "EdgeFNF: Toward real-time fake news detection on mobile edge computing," in Proc. 2022 Seventh Int. Conf. Fog Mob. Edge Comput. (FMEC), Paris, France, Dec. 12–15, 2022.