When Drone-Vehicle Networks Meets mmWave Communications: Current Status, Challenges, and Future Research Directions

Ye Liu, Honggang Wang, Yucheng Xie, and Ashikur Nobel

***Abstract*—The convergence of unmanned aerial vehicles and ground-based vehicles is driving the emergence of drone-vehicle networks, which promise transformative capabilities in autonomous mobility, emergency response, environmental monitoring, and smart city applications. To meet the stringent demands for high data rates and ultra-low latency in these dynamic environments, millimeter-wave (mmWave) communication has been identified as a key enabler. This article provides a comprehensive exploration of the mmWave-integrated drone-vehicle networks paradigm. We first conduct a bibliometric analysis to map the evolution and current trends in this emerging field, identifying key technologies and thematic research clusters. We then examine critical challenges that hinder dependable mmWave communication in such networks, focusing on three interdependent areas: accurate channel measurement and modeling, reliable communication link maintenance, and robust security mechanisms. To address these challenges, we propose a set of forward-looking research directions, including computational intelligence-based channel modeling, AI-empowered autonomous resource scheduling, adaptive and lightweight security frameworks, and the integration of large language models for enhanced network management. This article serves as a roadmap to guide future research and technological development in this promising area.**

I. Introduction

The rapid evolution of autonomous systems has increasingly led to the integration of ground-based vehicle networks and unmanned aerial vehicle (UAV) networks, forming new drone-vehicle networks (DVNs) [1]. These emerging networks represent a transformative architecture in intelligent autonomous mobile network systems, where drones and ground vehicles cooperate to enable joint sensing, distributed intelligence, and coordinated operations. By harnessing the aerial agility and wide-area visibility of drones alongside the stability and computational resources of ground vehicles, such networks offer enhanced situational awareness, broader coverage, and greater operational flexibility.

Concurrently, mmWave communication has emerged as a promising solution to meet the stringent bandwidth and latency requirements of drone-vehicle networks [2]. mmWave offers multi-gigabit per second data rates and ultra-low latency, making it well-suited for real-time sharing of high-volume sensor data such as video, LiDAR, and radar streams. These features are particularly advantageous in collaborative scenarios that demand rapid and reliable data exchange to support time-sensitive operations.

Ye Liu, Honggang Wang (corresponding author), Yucheng Xie, and Ashikur Nobel are with Katz School of Science and Health, Yeshiva University, USA.

However, integrating mmWave communication into drone-vehicle networks introduces substantial challenges, particularly concerning dependability. Here, dependability refers to the ability to maintain reliable and secure communication within such a dynamic and complex network environment. The main reasons lie in multiple aspects. *First*, the high-frequency nature of mmWave signals results in limited penetration and high susceptibility to blockage by obstacles such as trees, buildings, and even the vehicles themselves. This is especially problematic in dynamic three-dimensional (3D) environments, where both drones and vehicles are constantly in motion, leading to frequent topology changes and intermittent line-of-sight (LoS) conditions. *Second*, mmWave links rely heavily on directional beamforming, which requires accurate and rapid beam alignment. This process becomes increasingly difficult under high mobility, unpredictable trajectories, and rapidly changing channel conditions. *Third*, security vulnerabilities are amplified in mmWave-based drone-vehicle networks. The open-air propagation of mmWave signals, combined with beam-steering mechanisms, may expose the system to eavesdropping, beam spoofing, or jamming attacks.

Therefore, while mmWave communication provides the foundation for high-capacity networking in drone-vehicle systems, achieving dependable operation requires a holistic rethinking of wireless communication strategies and network protocol design. These challenges highlight critical research questions: *a)* How can intelligent, adaptive mmWave channel measurement and modeling frameworks be developed to effectively handle the complexity and dynamism inherent in drone-vehicle networks? *b)* How to enhance the reliability of mmWave communications under varying and adverse channel conditions? *c)* What strategies can ensure robust security measures that effectively protect drone-vehicle networks against emerging cybersecurity threats and vulnerabilities?

To this end, this article serves as both a comprehensive survey of the current state of mmWave-integrated drone-vehicle networks and a forward-looking perspective on promising future research directions. Specifically, we make the following key contributions:

- We conduct a bibliometric analysis of drone-vehicle networks, review the state-of-the-art in utilizing mmWave communications for these systems, and envision a future network paradigm.
- Building on bibliometric insights, we provide an in-depth discussion of challenges facing mmWave-integrated drone-vehicle networks in channel measurement and

modeling, reliable communication, and cybersecurity.
- To address these challenges, we propose several promising research directions, including computational intelligence-based methodologies, autonomous resource scheduling powered by artificial intelligence, robust security solutions, and the use of large language models for enhanced drone-vehicle network management.

The remainder of this article is organized as follows. First, a review and insights into drone-vehicle networks integrated with mmWave communications are presented. Next, key challenges are examined. Subsequently, future research directions are outlined. Finally, concluding remarks are provided.

II. Drone-Vehicle Networks

This section begins with a bibliometric analysis of drone-vehicle networks. Drawing on these findings, it envisions a future paradigm that leverages mmWave communications to enable a range of emerging applications.

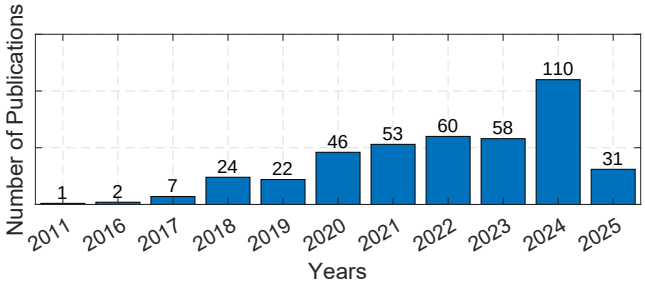
A. Bibliometric Analysis

1) Methodology: This study employs a combination of statistical analysis and bibliometric visualization to uncover key patterns and trends in the field. Statistical analysis was used to identify publication trends over time and analyze document types, offering a quantitative overview of research activity. Complementarily, bibliometric visualization using CiteSpace enabled an intuitive exploration of the field's geographical distribution, keyword co-occurrence, and research timelines. The motivation behind this approach is to systematically map the intellectual structure and evolution of mmWave-integrated drone-vehicle networks, supporting the identification of emerging research hotspots and potential future directions.

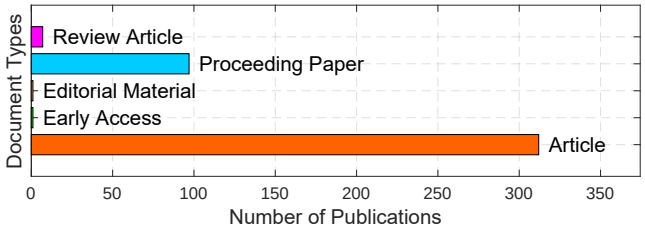
2) Data Source: The data were retrieved from the Web of Science Core Collection, covering a wide range of scholarly publications published between January 2011 and May 2025 (as of the manuscript preparation). Initial search queries combined the keywords "drone vehicle network," "drone assisted vehicular network," and "UAV assisted vehicular network" each separately with the keyword "mmWave," yielding 62, 1, and 8 papers respectively, resulting in a total of 71 papers. Due to the relatively low number of results, the keyword "mmWave" was subsequently excluded to broaden the search scope. This revised approach resulted in 25, 64, and 300 papers respectively. The final dataset comprising these papers provided a robust basis for conducting an in-depth analysis.

3) Statistical Results: The publication trends are presented in Fig. 1a, highlighting a clear upward trajectory in research activity over the examined period. The field experienced slow initial growth, with only a single publication in 2011. A notable increase began in 2018 (24 publications), accelerating substantially in subsequent years, peaking in 2024 with 110 publications. Although there is a decrease to 31 publications in 2025, this is due to incomplete data collection for the ongoing year at the time of manuscript preparation (May 2025).

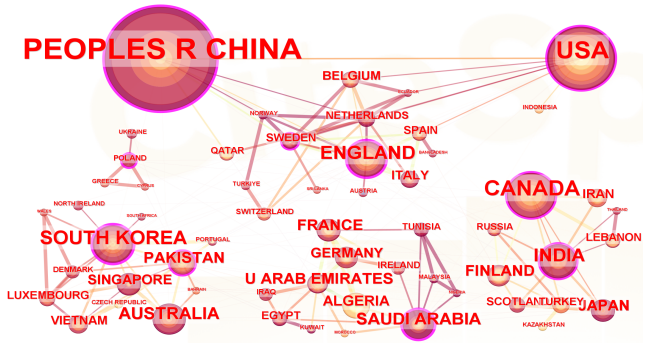
Fig. 1b illustrates document type distribution, indicating that the majority of scholarly output consists of original research articles (312 publications), followed by proceeding



(a) The Trend of Publications



(b) Document Type



(c) Geographical Distribution

Fig. 1. Statistical analysis and bibliometric visualization results of drone-vehicle networks research over the past years between January 2011 and May 2025 (as of the manuscript preparation).

papers (97). Review articles represent a smaller but significant portion, comprising seven publications, reflecting a mature field with ongoing synthesis of existing knowledge.

The geographical distribution of publications (Fig. 1c) shows significant international engagement in the research area. China dominates the publication landscape, accounting for 53.01% of all publications, followed by the USA (19.76%) and Canada (12.05%). Notably, other active countries include South Korea (7.23%), England (6.99%), and India (6.27%), indicating widespread global interest and collaboration in the drone-vehicle networks research domain. This diversity highlights the global relevance and broad interest across developed and emerging research communities.

B. Research Evolution Trends

1) Timeline of Co-Occurring Keywords in Drone-Vehicle Networks: As demonstrated in Fig. 2, several evolutionary trends have emerged clearly over the observed period. Early research primarily focused on fundamental aspects, such as ground-to-air channel characterization, optimizing communication networks, and exploring UAV-assisted vehicular sys-

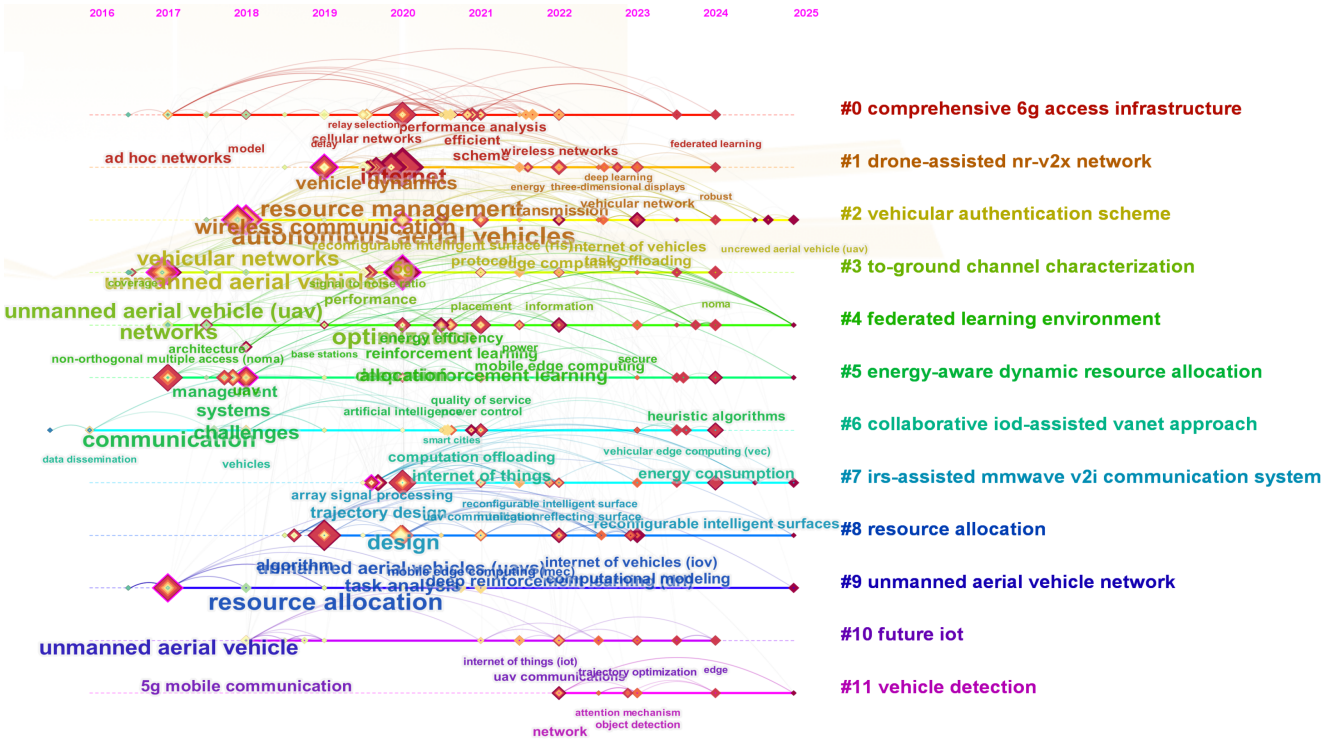


Fig. 2. Timeline of research progress and key technological developments in drone-vehicle networks over the past decade from January 2016 through May 2025 (the timeframe available at the time of manuscript preparation).

tems. These initial studies provided the necessary foundational knowledge to support more advanced, integrative research.

From around 2018 onwards, significant attention shifted toward comprehensive 6G access infrastructure, reflecting the industry's growing anticipation of next-generation communication technologies [3]. This period marked a substantial increase in research related to relay selection protocols and optimizing UAV-assisted Internet of vehicles (IoV) networks over licensed and unlicensed spectra. The evolution in the field saw a diversification in research topics from 2020 onwards. Digital twins [4], federated learning environments [5], and Intelligent Reflecting Surface (IRS)-aided communication systems emerged prominently, signifying a shift towards integrating advanced computational intelligence techniques into UAV and vehicular communication systems [6]. More recently, the focus has intensified around vehicle authentication schemes [7], collaborative Internet of Drones (IoD)-assisted approaches, and energy-aware dynamic resource allocation strategies, underscoring an increased priority on security, collaborative network efficiency, and sustainability [8]. Furthermore, reinforcement learning and IRS-assisted mmWave communication systems became central themes, highlighting the increasing complexity and sophistication of current research methodologies [9].

Overall, the field's evolution reflects a clear trajectory from fundamental explorations of UAV-enabled vehicular networks towards complex, integrative systems leveraging advanced machine learning, sophisticated resource management, and sustainable and secure communication practices.

2) Keywords Co-occurrence Clustering in mmWave-Integrated Drone-Vehicle Networks: To dive deeper into the research focus on integrating mmWave communication into drone-vehicle networks, we further conducted a keyword co-occurrence clustering analysis. It was based on 69 unique papers obtained after removing duplicates from the initial pool of 71 papers. Using CiteSpace, we examined keyword co-occurrence patterns, which revealed several prominent research clusters that help map the intellectual structure of the field. Eight main groups emerged, each representing a different thematic area, as shown in Fig. 3.

a) Cellular-Connected Drone Corridor: The largest cluster focuses on cellular-connected drone corridors, indicative of significant research interest in creating reliable communication pathways for drones leveraging cellular networks, especially emphasizing mmWave links for minimizing ground risks [10]. This cluster prominently features performance analysis, 5G mobile communication, and autonomous aerial vehicles.

b) Tethered Drone Access and Backhaul Network: Another significant cluster explores tethered drone-assisted integrated access and backhaul networks [11]. Here, the primary emphasis is on optimizing network designs using non-orthogonal multiple access and innovative approaches involving drone-assisted backhaul solutions, revealing a strong trend toward enhancing communication efficiency and coverage.

c) Open Research Topics: Research topics identified as open and prospective constitute an important cluster, suggesting active exploration into emerging technologies and future research directions [12]. This includes empowering heterogeneous communication data links and leveraging intelligent reflecting surfaces, marking a forward-looking stance.

d) UAV Cellular Communication: This forms another vital cluster with research pivoting towards integrating UAV

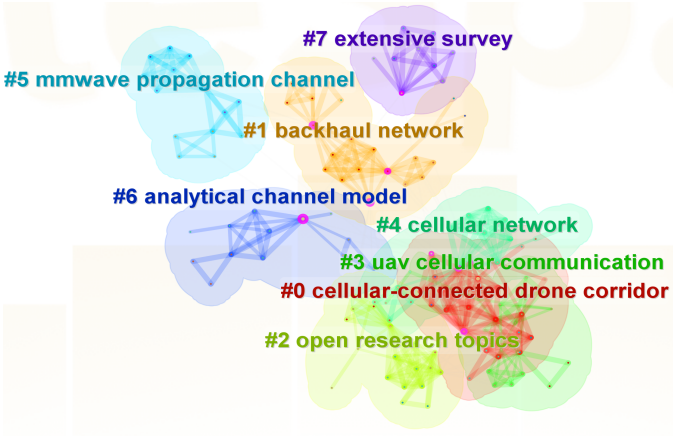


Fig. 3. Clustering of keyword co-occurrences to reveal core research themes in mmWave-integrated drone-vehicle networks.

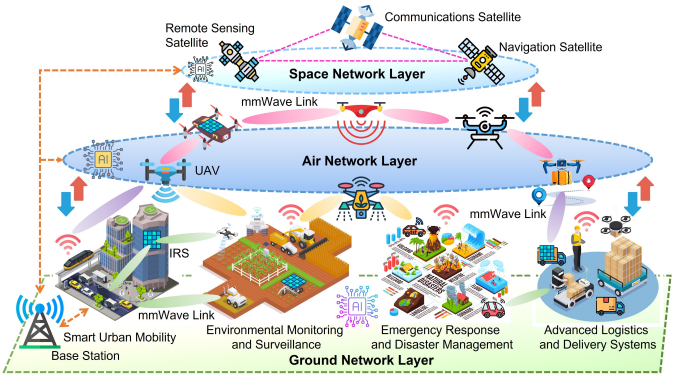


Fig. 4. Future paradigm of mmWave-integrated drone-vehicle networks.

systems within cellular frameworks and addressing associated security threats [13]. This area underscores the critical importance of secure, high-capacity communication systems in increasingly mobile and dynamic environments.

e) mmWave Propagation Channel and Analytical Model: Clusters dedicated to mmWave propagation characteristics and analytical channel models highlight rigorous explorations into channel modeling, ray tracing, and propagation studies [14]. These efforts lay the foundation for enhancing communication reliability and performance in dense urban and built-up environments where drone-vehicle networks are deployed.

f) Extensive Survey and Cellular Network: The comprehensive survey and cellular network clusters emphasize a synthesis of knowledge and empirical analyses of cellular network performance, particularly focusing on 5G-connected drones and content delivery via aerial caching. These clusters reflect a deep integration of empirical research and theoretical frameworks aimed at optimizing the performance and deployment of advanced communication technologies.

Collectively, these clusters delineate a vibrant and diverse research landscape in mmWave-integrated drone-vehicle networks, reflecting both foundational theoretical investigations and applied research aimed at solving practical challenges.

C. mmWave-Integrated Drone-Vehicle Networks

Insights from the bibliometric analysis reveal a clear trajectory toward more sophisticated network architectures that integrate mmWave technology with drone-vehicle networks. In the following, we envision this future network paradigm.

1) Future Network Paradigm: As shown in Fig. 4, the envisioned future network architecture of mmWave-integrated drone-vehicle networks adopts a multi-layered hierarchical design in which the Ground, Air, and Space layers are not isolated, but interdependent and mutually reinforcing.

At the ground network layer, smart urban mobility base stations, terrestrial vehicles, and IoT devices form the foundation of connectivity. These nodes generate massive amounts of real-time data from diverse domains such as traffic management, environmental monitoring, and logistics. However, due to the limited coverage and frequent blockages of mmWave links, relying solely on ground connectivity is insufficient. The air network layer acts as a highly mobile bridge between ground and space. UAVs dynamically reposition themselves to extend coverage, relay traffic from obstructed terrestrial users, and provide low-latency links for mission-critical services. Moreover, UAVs can aggregate heterogeneous ground data and offload it upward to satellites or laterally to other UAVs, thereby balancing network loads. At the space network layer, remote sensing, navigation, and communication satellites provide stable global backhaul connectivity. Satellites ensure long-distance, delay-tolerant communication and deliver essential services such as localization, synchronization, and environmental awareness. They also support UAV swarms by enabling wide-area coordination and resilience when terrestrial infrastructure is unavailable or damaged.

Importantly, these three layers form a closed feedback loop. Ground data (traffic flow, environmental events) informs UAV deployment strategies. UAV relays maintain continuity of mmWave links and aggregate data upward. Satellites distribute global information (e.g., navigation, disaster alerts) back to both UAVs and ground stations. The network is further empowered by advanced technologies such as intelligent reflecting surfaces (IRS) to manipulate wireless channels, AI-driven decision-making for adaptive resource allocation, and digital twin paradigms for real-time simulation of cross-layer behaviors. Together, these elements enable seamless integration, enhance reliability and scalability, and ensure that the overall system can flexibly adapt to dynamic environments.

2) Distinct Advantages: The proposed mmWave-integrated drone-vehicle networks offer substantial advantages over traditional communication and networking paradigms across multiple aspects, as summarized in Table I.

- **Coverage:** Extensive 3D coverage refers to seamless connectivity across both aerial and terrestrial domains, providing significantly broader and more continuous service than ground-only or air-only networks.
- **Bandwidth:** High (multi-Gbps capability) highlights the potential of mmWave frequencies to deliver multi-gigabit data rates, compared to the sub-Gbps capacity typical of traditional networks.
- **Latency:** Ultra-low latency denotes end-to-end communication delay in the millisecond range, made possible

TABLE I
COMPARISON OF MMWAVE-INTEGRATED DRONE-VEHICLE NETWORKS WITH OTHER APPROACHES ACROSS KEY ASPECTS

Aspect	mmWave-integrated Drone-Vehicle Networks	Traditional Ground Vehicle Networks	Traditional UAV Networks	Traditional Wireless Drone-Vehicle Networks
Coverage	Extensive 3D coverage (ground & air)	Limited ground-only coverage	Limited aerial-only coverage	Improved but limited coverage
Bandwidth	High (multi-Gbps capability)	Limited (sub-Gbps)	Moderate (sub-Gbps)	Moderate (sub-Gbps)
Latency	Ultra-low latency due to direct mmWave links	Higher latency due to limited direct connectivity	Moderate latency	Moderate latency
Mobility & Flexibility	Highly flexible, dynamically adaptable network topology	Low flexibility, limited adaptability due to infrastructure	High mobility but limited scalability	Moderate flexibility and scalability
Reliability & Security	Enhanced through advanced technologies	Moderate security, vulnerable to physical disruptions	Moderate security with limited reliability	Moderate, limited by conventional techniques

Note: Descriptive terms in this table are defined relative to conventional wireless technologies. "Extensive 3D coverage" denotes integrated ground–air connectivity, "multi-Gbps capability" indicates the achievable peak data rate enabled by mmWave frequencies, and "ultra-low latency" refers to end-to-end delays on the order of milliseconds. Similarly, "high mobility and flexibility" highlights dynamic UAV repositioning for adaptive topologies, while "enhanced reliability and security" reflects the use of IRS, AI, and digital twins to ensure resilience against disruptions and threats.

by direct line-of-sight mmWave links while conventional systems often rely on multihop paths that increase latency.

- **Mobility & Flexibility:** This reflects the ability of UAVs to dynamically reposition and reconfigure topologies on demand, in contrast to fixed terrestrial infrastructures or scalability-limited UAV-only systems.
- **Reliability & Security:** Enhanced performance captures the added robustness from emerging technologies such as intelligent reflecting surfaces (IRS), AI-driven control, and digital twins, which collectively strengthen resilience against both physical disruptions and cyber threats.

III. CHALLENGES IN MMWAVE-INTEGRATED DRONE-VEHICLE NETWORKS

Despite its promising potential, research on mmWave-integrated drone-vehicle networks is still in its early stages. As revealed by our bibliometric analysis, existing studies primarily focus on three fundamental challenges: channel measurement and modeling, reliable communication links, and network security. Here, we discuss these challenges in detail.

A. Channel Measurement and Modeling

Accurate channel measurement and modeling are fundamental to dependable mmWave communication in drone–vehicle networks, yet they remain highly challenging. Although recent advances such as mixed deterministic–stochastic modeling and real-time digital twin (DT)–based approaches have improved fidelity, they cannot fully capture the complexity of aerial–terrestrial environments.

In practice, drone–vehicle scenarios involve simultaneous mobility of UAVs and ground vehicles, producing intricate Doppler effects, rapid LoS/NLoS transitions, and frequent blockages that cause abrupt variations in link quality. These dynamics are further compounded by spatial–temporal heterogeneity, where propagation conditions differ significantly across urban canyons, highways, and open fields. Additionally, mmWave signals are extremely sensitive to atmospheric factors such as rain, fog, and humidity, requiring fine-grained modeling that is difficult to achieve consistently. Despite progress, most models remain scenario-specific, with limited transferability across environments, and large-scale, synchronized air–ground measurement datasets are still scarce.

Together, these factors make channel measurement and modeling a persistent challenge in realizing reliable and generalizable mmWave-integrated drone–vehicle networks.

B. Reliable Communication Links

Reliable communication is the backbone of drone–vehicle networks, yet ensuring it under the stringent requirements of mmWave systems remains highly challenging. The inherent vulnerability of mmWave links to blockage and attenuation leads to frequent link intermittency, as independently moving drones and vehicles encounter sudden obstructions and rapidly changing topologies. Directional transmission further complicates the problem as narrow beams require continuous tracking and alignment, which is difficult to achieve with sufficient responsiveness in high-mobility 3D environments. At the same time, diverse applications impose heterogeneous Quality of Service (QoS) requirements, ranging from ultra-reliable low-latency control to bandwidth-intensive video streaming, but current protocols struggle to provide differentiated guarantees in fast-varying conditions. These issues are compounded by the lack of effective cross-layer coordination such as link margin, Doppler shifts, and interference directly impact throughput, latency, and reliability at higher layers, yet protocol designs often treat these layers in isolation.

Combined, these factors make the design of adaptive and energy-efficient mmWave communication for drone–vehicle networks a persistent and multifaceted challenge.

C. Network Security

The security of mmWave-integrated drone–vehicle networks is critical yet remains underexplored, despite their envisioned use in mission-critical and safety-sensitive applications such as emergency response and intelligent transportation systems. First, the introduction of high-mobility nodes and directional mmWave links expands the attack surface, exposing vulnerabilities across multiple dimensions. From an availability

perspective, denial-of-service (DoS) and energy-draining attacks can severely disrupt connectivity. Second, in terms of integrity, spoofing, replay, and route manipulation threaten the correctness of control and data flows. Third, confidentiality is at risk from targeted eavesdropping or beam sniping, while authenticity and trust are undermined by Sybil attacks and identity spoofing. Side-channel vulnerabilities may arise from leakage through beam patterns, timing, or RF emissions.

These diverse threats are exacerbated by dynamic topology changes and frequent handovers, which render conventional centralized authentication or static cryptographic schemes impractical due to latency and computational costs. Moreover, the high-value nature of transmitted data, including control commands, sensor streams, and video, magnifies the consequences of compromised confidentiality or integrity. Although physical-layer techniques such as secure beamforming, artificial noise, or IRS-assisted obfuscation show promise, most remain theoretical and lack validation under realistic mobility and environmental conditions. Compounding these issues is the absence of formal threat models, quantified risk assessments, and systematic taxonomies, which makes it difficult to evaluate vulnerabilities or compare defenses across different attack scenarios.

In summary, these factors highlight that security in mmWave-integrated drone–vehicle networks is a multidimensional and unresolved challenge that must be addressed as an integral part of reliable system design.

D. Interconnected Challenges

The challenges of channel measurement, reliable communication, and network security are deeply interrelated rather than independent. Accurate channel models provide the foundation for predicting link quality, but their limitations directly affect the design of reliable protocols. At the same time, ensuring link reliability requires cross-layer adaptability, yet frequent beam realignments and intermittent connectivity expose new security vulnerabilities. Furthermore, the computational and energy overheads of reliability and security mechanisms are tightly coupled with the constraints of UAVs and vehicles, where limited resources magnify trade-offs between performance, efficiency, and protection. In addition, failures in one dimension often cascade into others. For example, poor channel estimation can reduce link stability, which in turn weakens authentication and trust.

Taken together, these interactions highlight the need for novel approaches that address measurement, reliability, and security to realize dependable mmWave-integrated drone–vehicle networks.

IV. Future Research Directions

To address the challenges outlined above and unlock the full potential of mmWave-integrated drone-vehicle networks, this section presents key directions for future research, as summarized in Fig. 5.

A. Computational Intelligence-Based Channel Modeling

To develop accurate and generalizable mmWave channel models for drone-vehicle networks, a comprehensive, multi-phase methodology is essential. Traditional empirical or geometry-based modeling approaches fall short in capturing the complex, dynamic, and heterogeneous conditions inherent to 3D aerial-ground environments. Computational intelligence offers a promising paradigm to overcome these limitations by learning intricate channel behaviors directly from measured data. The research involves four key phases:

1) Measurement Campaign and Data Acquisition: This focuses on conducting real-world measurement campaigns across diverse scenarios (e.g., urban canyons, open fields, highway corridors). Both aerial and vehicular platforms are equipped with mmWave transceivers to capture spatial, temporal, and frequency-domain data under varying mobility, altitude, and environmental conditions.

2) Data Processing and Feature Engineering: Raw measurement data is noisy and unstructured. Signal denoising, synchronization, and data alignment are performed as preprocessing steps. Then, relevant features such as Doppler shifts, delay spreads, angle-of-arrival, and received signal strength are extracted and structured to represent channel dynamics.

3) Computational Intelligence-Based Modeling: Machine learning and recurrent architectures can be employed to learn the underlying mapping between mobility, environmental features, and channel parameters. These models can capture nonlinear dependencies, adaptive beam behaviors, and real-time channel evolution patterns that conventional models overlook.

4) Validation and Generalization: To ensure reliability and robustness, models should be validated on unseen environments and cross-scenario test datasets. Generalization techniques, such as transfer learning or domain adaptation, can be explored to extend trained models across different geographic regions and operational conditions.

B. AI-Empowered Autonomous Resource Scheduling

In dynamic and mission-critical drone-vehicle networks, maintaining reliable mmWave communication requires continuous adaptation of communication resources. Manual or rule-based scheduling strategies often lack the responsiveness and scalability to handle the stochastic and time-varying nature of such environments. Therefore, future research should focus on autonomous, AI-driven resource scheduling frameworks. Key aspects of this direction include:

1) Reinforcement Learning for Link and Beam Management: Reinforcement learning (RL) offers an effective solution for link and beam management in mmWave drone-vehicle networks, where mobility, blockage, and channel variability challenge static or model-based strategies. Unlike conventional methods, RL learns optimal policies through continuous interaction, making it well-suited for dynamic, uncertain environments. RL agents adaptively manage beam alignment, link association, and scheduling by optimizing long-term performance metrics such as throughput, latency, and reliability. Its scalability to high-dimensional, multi-agent scenarios makes RL a strong candidate for complex, real-time decision-making in coordinated drone-vehicle communications.

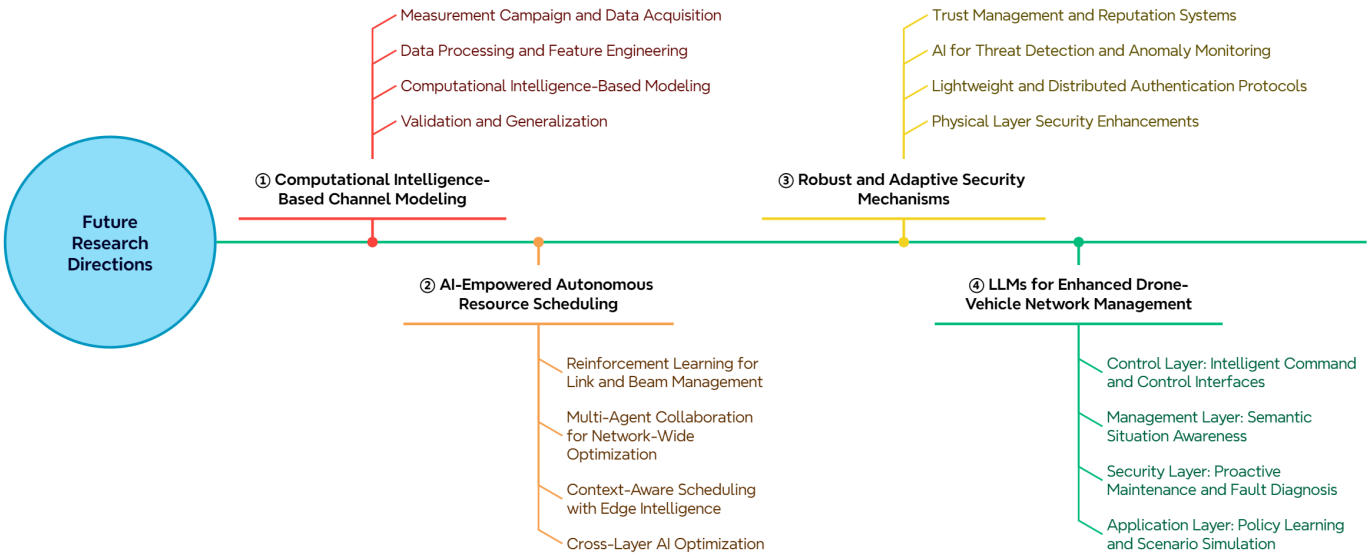


Fig. 5. Future research directions for mmWave-integrated drone-vehicle networks.

2) Multi-Agent Collaboration for Network-Wide Optimization: In multi-drone and multi-vehicle scenarios, decentralized AI agents can collaborate to optimize network-wide objectives such as throughput, latency, or fairness. Multi-agent reinforcement learning enables distributed decision-making while minimizing signaling overhead and avoiding conflicts.

3) Context-Aware Scheduling with Edge Intelligence: Edge computing platforms onboard drones or vehicles can host lightweight AI models for real-time inference and scheduling decisions. By leveraging local context (e.g., position, velocity, channel state), the system can achieve ultra-low-latency adaptation without centralized bottlenecks.

4) Cross-Layer AI Optimization: Integrating AI-driven decision-making across multiple layers of the network stack (i.e., the Physical (PHY), Medium Access Control (MAC), and Network layers) enables holistic, end-to-end optimization for communication performance. Traditional layered architectures often suffer from suboptimal coordination, where decisions made independently at each layer can conflict or overlook cross-layer dependencies. In contrast, AI models can jointly learn and adapt policies that align physical-layer parameters with MAC-layer strategies and network-layer goals.

For example, when an AI agent predicts an imminent blockage at the PHY layer based on channel state information or mobility cues, it can proactively adjust the direction or beamwidth of the beam while, at the same time, adapting the MAC-layer retry strategy and reassigning the link association to minimize packet loss. Similarly, if the AI agent detects QoS-critical flows (e.g., low-latency control signals), it can prioritize them by coordinating PHY resource blocks with MAC scheduling policies. This cross-layer intelligence ensures that physical-layer adjustments, medium access decisions, higher-layer routing, and QoS reinforce rather than conflict with one another, thus enhancing robustness, efficiency, and service differentiation in mmWave-integrated drone–vehicle networks.

C. Robust and Adaptive Security Mechanisms

Ensuring the security of mmWave-integrated drone–vehicle networks requires next-generation mechanisms that are lightweight, adaptive, and validated under real-world mobility and resource constraints. Future research should therefore focus on practical designs that balance feasibility, scalability, and resilience against evolving threats, as outlined below.

1) Physical-Layer Security Enhancements: Physical-layer techniques leverage the inherent directionality and randomness of mmWave propagation to provide secrecy without heavy cryptographic overhead. For example, secure beamforming can dynamically steer beams toward legitimate receivers while minimizing side-lobe leakage that may expose signals to eavesdroppers. Cooperative jamming can be made practical by assigning UAV relays to inject controlled interference that selectively degrades an adversary's reception while preserving the legitimate link's signal-to-interference ratio (SIR). Artificial noise injection, tailored to the estimated channel state, can further enhance secrecy capacity in environments where beam interception is likely. Future work should quantify these techniques under realistic UAV mobility patterns and multi-beam scenarios, focusing on metrics such as secrecy outage probability, energy cost of jamming, and trade-offs between link reliability and confidentiality.

2) Lightweight and Distributed Authentication Protocols: Frequent handovers and dynamic topologies make traditional centralized authentication unsuitable for mmWave-integrated drone–vehicle networks. Lightweight schemes based on elliptic-curve cryptography or hash-chain verification can reduce computational and communication overhead, enabling authentication within a few milliseconds. In highly mobile scenarios, blockchain-inspired ledgers distributed across UAVs or roadside units could provide decentralized trust anchors, but their feasibility depends on minimizing consensus delay. Future work should design hybrid schemes that combine fast local authentication (e.g., physical unclonable functions and one-time tokens) with periodic global verification, and evalu-

ate them against performance metrics such as authentication latency, overhead per session, and robustness to attacks.

3) AI for Threat Detection and Anomaly Monitoring: AI-based intrusion detection offers the potential to identify both known and novel attacks by analyzing fine-grained features from control traffic, PHY-layer signals, and UAV mobility patterns. For instance, a machine learning model could distinguish normal beam-alignment behavior from malicious jamming by monitoring abnormal signal-to-noise ratio or Doppler profiles. Unsupervised or semi-supervised methods are particularly suitable for detecting zero-day threats, while federated learning could allow UAVs to collaboratively train detectors without centralizing sensitive data. Key research challenges include adversarial robustness (ensuring attackers cannot fool the detectors), model efficiency (keeping inference within UAV computational budgets), and validation on realistic datasets.

4) Trust Management and Reputation Systems: In semi-trusted environments, node misbehavior (such as selective forwarding, false reporting, or excessive retransmissions) can degrade network performance and security. Trust management frameworks should assign reputation scores based on direct observations (e.g., packet delivery ratio, beam alignment reliability) and indirect evidence propagated by peers. To remain practical, these systems must be lightweight, resistant to collusion, and capable of rapid adaptation to changing mobility patterns. Techniques such as Bayesian updating or reinforcement learning can enable dynamic trust adjustment, while integration with blockchain-based ledgers may provide tamper-resistant records of behavior. Feasibility studies should evaluate these systems using metrics such as trust convergence time, resilience under collusion attacks, and overhead in terms of signaling and computation.

D. LLMs for Enhanced Drone–Vehicle Network Management

Large Language Models (LLMs), such as ChatGPT, LLaMA, Falcon, and domain-adapted variants like DistilBERT, offer transformative capabilities for contextual reasoning, semantic understanding, and human–machine interaction. While encoder-style models (e.g., BERT, DistilBERT) excel at classification and contextual analysis, decoder-style models (e.g., GPT-4/5, LLaMA-2, Falcon) are designed for generative reasoning and adaptive dialogue, making them well-suited for dynamic instruction synthesis and interactive control. Leveraging both types in complementary roles can enhance semantic awareness, decision support, and mission-level coordination in mmWave-enabled drone–vehicle networks.

1) Feasibility: Running full-scale LLMs directly on UAV or vehicle hardware is computationally infeasible due to memory, latency, and energy constraints. Practical deployments must therefore rely on hybrid strategies. Heavy inference can be offloaded to edge or cloud nodes, while lightweight distilled or quantized variants (e.g., DistilGPT-2, TinyBERT, and LoRA-based models) operate locally for time-critical decisions. Techniques such as model pruning, parameter sharing, and on-device caching further reduce latency, enabling partial inference on UAVs while preserving global reasoning at the edge.

2) Integration Strategies: To move beyond broad claims, LLMs can be mapped to specific layers of the drone–vehicle network architecture:

- *Control Layer:* Natural-language interfaces where operators issue high-level mission instructions that LLMs translate into protocol-compliant control commands.
- *Management Layer:* Semantic analysis of telemetry logs, mobility traces, and network status to detect anomalies (e.g., blockage prediction, route instability).
- *Security Layer:* Policy learning and adversarial simulation, where LLMs generate candidate attack scenarios or validate defenses when integrated with reinforcement learning and digital twin environments.
- *Application Layer:* Contextual prioritization of heterogeneous QoS flows (e.g., distinguishing urgent safety-critical control from bulk video streaming).

Recent works [15] have begun exploring LLMs for network control and security, showing their potential in space-air-ground integrated network. In summary, by combining full-scale LLMs at the edge/cloud with lightweight variants embedded on UAVs, and by explicitly mapping their functions to control, management, security, and application layers, future research can transform LLMs from a conceptual idea into a technically grounded framework for dependable drone–vehicle network management.

V. Conclusion

As the demand for intelligent, autonomous, and collaborative systems continues to grow, drone–vehicle networks have emerged as a powerful paradigm to address the complexities of modern communication and sensing in dynamic environments. Integrating mmWave communication into such networks unlocks the potential for ultra-high-speed, low-latency data exchange. However, the deployment of mmWave-integrated drone–vehicle networks remains in its nascent stage, facing significant challenges related to channel dynamics, link reliability, and cybersecurity. Through a comprehensive bibliometric analysis and synthesis of the state of the art, this article has provided a foundational understanding of the current research landscape. Moreover, we have identified the major challenges impeding the dependable operation of these networks and outlined four pivotal future research directions.

In addition, it is important to acknowledge certain limitations of this survey-oriented work. First, while this work highlights architectural concepts and AI-based strategies, it does not provide baseline performance estimates (e.g., link margin under blockage, range–throughput trade-offs) or case studies that could validate these proposals. Incorporating such quantitative assessments in future work will be essential for substantiating design feasibility. Second, some critical challenges go beyond our observations and require deeper investigation. In particular, the high power consumption of mmWave hardware remains one of the most fundamental barriers to practical deployment, especially for UAVs with limited energy budgets. Similarly, the co-design of phased-array antennas with the physical structure of drones or vehicles introduces unique constraints in terms of aerodynamics, drag,

weight distribution, and thermal management, which must be systematically addressed. Addressing these deeper technical issues through both simulation-based evaluation and experimental prototyping will be crucial to move the field from conceptual frameworks toward practical, deployable mmWave-integrated drone–vehicle networks.

ACKNOWLEDGMENT

The authors would like to express their sincere gratitude to anonymous reviewers for their valuable suggestions.

REFERENCES

[1] V. Beliautsou, A. Beliautsou *et al.*, "Drone-to-Vehicle Integration of Data: Design Concept and Application to Vehicle Automation System," *IEEE Vehicular Technology Magazine*, pp. 2–11, 2025.

[2] J. Tan, T. H. Luan *et al.*, "Beam Alignment in mmWave V2X Communications: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 26, no. 3, pp. 1676–1709, 2024.

[3] Y. Su, L. Huang *et al.*, "Joint Power Control and Time Allocation for UAV-Assisted IoV Networks Over Licensed and Unlicensed Spectrum," *IEEE Internet of Things Journal*, vol. 11, no. 1, pp. 1522–1533, 2024.

[4] B. Hazarika, K. Singh *et al.*, "RADiT: Resource Allocation in Digital Twin-Driven UAV-Aided Internet of Vehicle Networks," *IEEE Journal on Selected Areas in Communications*, vol. 41, no. 11, pp. 3369–3385, 2023.

[5] P. Du, T. Xiao *et al.*, "Energy-Efficient Drones and BS Management in Distributed Edge Intelligence Empowered IoV Networks," *IEEE Internet of Things Journal*, vol. 12, no. 5, pp. 4667–4680, 2025.

[6] A. C. Pogaku, D.-T. Do *et al.*, "UAV-Assisted RIS for Future Wireless Communications: A Survey on Optimization and Performance Analysis," *IEEE Access*, vol. 10, pp. 16 320–16 336, 2022.

[7] Z. Guo, J. Cao *et al.*, "UAVA: Unmanned Aerial Vehicle Assisted Vehicular Authentication Scheme in Edge Computing Networks," *IEEE Internet of Things Journal*, vol. 11, no. 12, pp. 22 091–22 106, 2024.

[8] S. Goudarzi, S. Ahmad Soleymani *et al.*, "Optimizing UAV-Assisted Vehicular Edge Computing With Age of Information: An SAC-Based Solution," *IEEE Internet of Things Journal*, vol. 12, no. 5, pp. 4555–4569, 2025.

[9] J. Yan, X. Zhao *et al.*, "Deep-Reinforcement-Learning-Based Computation Offloading in UAV-Assisted Vehicular Edge Computing Networks," *IEEE Internet of Things Journal*, vol. 11, no. 11, pp. 19 882–19 897, 2024.

[10] S. Singh, M. L. Sichitiu *et al.*, "Minimizing Ground Risk in Cellular-Connected Drone Corridors With mmWave Links," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 59, no. 6, pp. 7923–7937, 2023.

[11] Y. Zhang, M. A. Kishk *et al.*, "Deployment Optimization of Tethered Drone-Assisted Integrated Access and Backhaul Networks," *IEEE Transactions on Wireless Communications*, vol. 23, no. 4, pp. 2668–2680, 2024.

[12] L. Bariah, L. Mohjazi *et al.*, "A Prospective Look: Key Enabling Technologies, Applications and Open Research Topics in 6G Networks," *IEEE Access*, vol. 8, pp. 174 792–174 820, 2020.

[13] M. M. Azari, S. Solanki *et al.*, "Evolution of Non-Terrestrial Networks From 5G to 6G: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 4, pp. 2633–2672, 2022.

[14] M. T. Dabiri, H. Safi *et al.*, "Analytical Channel Models for Millimeter Wave UAV Networks Under Hovering Fluctuations," *IEEE Transactions on Wireless Communications*, vol. 19, no. 4, pp. 2868–2883, 2020.

[15] X. Cao, G. Nan *et al.*, "Exploring LLM-Based Multi-Agent Situation Awareness for Zero-Trust Space-Air-Ground Integrated Network," *IEEE Journal on Selected Areas in Communications*, vol. 43, no. 6, pp. 2230–2247, 2025.

Ye Liu received the M.S. and Ph.D. degrees in electronic science and engineering from Southeast University, China, in 2013 and 2018, respectively. He was a Visiting Scholar with Montana State University, USA from October 2014 to October 2015. He was a joint Ph.D. Student from February 2017 to January 2018 with the Networked Embedded Systems Group, RISE Swedish Institute of Computer Science. He was a Macau Young Scholar with Macau University of Science and Technology, Macau SAR, China, and a researcher with Nanjing Agricultural University, China. His current research interests include battery-free Internet of Things, tiny machine learning, and autonomous mobile networks.

Honggang Wang is the founding Chair and Professor of the Department of Graduate Computer Science and Engineering, Katz School of Science and Health, Yeshiva University in New York City. He is an alumnus of NAE Frontiers of Engineering program. He produced high-quality publications in prestigious journals and conferences in his research areas, winning several prestigious best paper awards. He is an IEEE distinguished lecturer and a Fellow of IEEE and AAIA. He has served as the Editor in Chief (EiC) for IEEE Internet of Things Journal during 2020–2022. He was the past Chair (2018–2020) of IEEE Multimedia Communications Technical Committee and the past IEEE eHealth Technical Committee Chair (2020–2021).

Yucheng Xie is an Assistant Professor in the Department of Graduate Computer Science and Engineering at the Katz School of Science and Health, Yeshiva University, New York City. He received his Ph.D. in Electrical and Computer Engineering from Purdue University and his M.S. in Computer Science from Stevens Institute of Technology. His research interests include wireless sensing, mobile computing, and security in machine learning and AI systems. His work has appeared in leading conferences and journals and has received multiple Best Paper and Runner-up Awards.

Ashikur Nobel is a doctoral candidate in the Department of Mathematics at the Katz School of Science and Health, Yeshiva University, where he also serves as a Research Assistant. He holds a Master's degree in Cybersecurity from Southeast Missouri State University. He has contributed to scholarly journals, including the ACM Health Journal and the IEEE Internet of Things Journal, with research in Generative AI and Wireless Communication. His research interest include developing AI-driven solutions for generative modeling of longitudinal and time-series sensor data, with applications in healthcare, drone-vehicle networks and the Internet of Things (IoT).