Received: 30 May 2024 | Revised: 4 September 2024 | Accepted: 27 September 2024

IET Intelligent Transport Systems

DOI: 10.1049/itr2.12579

The Institution of Engineering and Technology WILEY

REVIEW

Facets of security and safety problems and paradigms for smart aerial mobility and intelligent logistics

Simeon Okechukwu Ajakwe[1] | **Dong-Seong Kim**[2]

[1]Information and Communication Technology Convergence Research Centre, Kumoh National Institute of Technology, Gumi, South Korea

[2]Department of IT Convergence Engineering, School of Electronics Engineering, Kumoh National Institute of Technology, Gumi, South Korea

Correspondence
Dong-Seong Kim, Department of IT Convergence Engineering, School of Electronics Engineering, Kumoh National Institute of Technology, Gumi, South Korea.
Email: dskim@kumoh.ac.kr

Funding information
NRF; MSIT, Grant/Award Number: IITP-2024-RS-2020-II201612; MEST, Grant/Award Number: 2018R1A6A1A03024003; Ministry of Science and ICT, Grant/Award Number: IITP-2024-2022-00156394

Abstract

The use of unmanned aerial vehicles (UAVs) for smart and speedy logistics is still relatively nascent compared to traditional delivery methods. However, it is witnessing sporadic and steady growth due to booming demands, technological advancement, and regulatory support. The intelligence and integrity of UAV systems depend largely on the underlying cognitive and cybersecurity models, which serve as both eyes and brains to perceive and respond to the myriad of scenarios around them. Smart mobility and intelligent logistic ecosystems (SMiLE) are complex and advanced technological networks which are exposed to several issues. The incorporation of UAVs for priority logistics, thereby extending the coverage and capacity of SMiLE, further heightens these vulnerabilities and questions its security, safety, and sustainability. This review scrutinizes the significant security disruptions, smartness dynamics, and sundry developments for the sustainable deployment of UAVs as an aerial logistics-based vehicle. Using the PRISMA-SPIDER methodology, 157 articles were selected for quantitative analysis and 20 review articles for qualitative evaluation. Security and safety issues in UAVs cut across all the layers of logistics operations: components, communication, network architecture, navigation, supply chain etc. Expanding the capacity of SMiLE using UAV demands an intentional and incremental convergence-based integration of an agile explainable artificial framework for reliable and safety-conscious smart mobility, a scalable and tamperproof blockchain for multi-factor authentication, and a zero trust cybersecurity paradigm for inclusive enterprise-based authorization.

1 | INTRODUCTION

Smart mobility refers to integrating information and communication technologies (ICT) into various transportation modes and services to enhance the efficiency, safety, and sustainability of the systems [1]. According to authors [2], smart mobility is one of the eight cardinal factors for establishing a smart city. It includes technologies such as global positioning system (GPS), real-time traffic information, vehicle-to-vehicle (V2V), and vehicle-to-infrastructure (V2I) communication, as well as innovations in electric and autonomous vehicles. On the other hand, an intelligent logistic ecosystem encompasses the interconnected network of systems, engineering, technologies, and social complexities involved in the planning, management, and execution of logistics operations [3]. This includes supply chain management software, tracking and tracing systems, predictive analytics, and other tools that optimize the movement of goods from production to consumption, with a focus on reducing costs, improving reliability, and minimizing environmental impact. Thus, smart mobility and intelligent logistic ecosystem (SMiLE) aim to create seamless and efficient transportation and logistics networks that leverage data and technology to address challenges such as congestion, pollution, and inefficient resource utilization. SMiLE enables real-time monitoring, decision-making, and optimization, leading to more sustainable and resilient transportation and logistics systems with 360-degree technological coverage [4].

The rising deployment of unmanned aerial vehicles (UAVs), especially drones, to achieve SMiLE, expand network connectivity, and access difficult terrains is attracting global attention. This is due to enormous benefits, such as green logistics, speedy delivery, scalable flexibility, cost-effectiveness, etc. associated

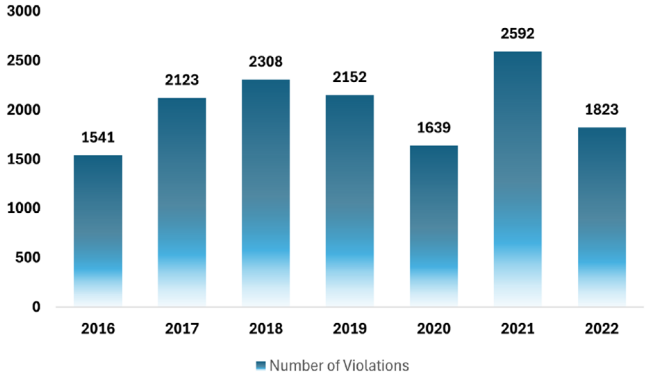

FIGURE 1 Number of UAV-related violations in the United States between 2016 and 2022 as reported by the Federal Aviation Administration (FAA).

with UAV usage. Authors [5] stated that the estimated number of registered drone users in the United States (US) by 2022 is around 2.4 million, of which 318,000 are commercial drone operators. However, the rising incidences of security breaches, unauthorized usage, and coordinated attacks carried out using UAVs cast doubt on the viability and reliability of UAVs' networks, intelligence, and security frameworks, coupled with protracted legislation on the use of civil drones in the airspace [6]. For instance, the Federal Aviation Administration (FAA) recorded 14718 cases of UAV-related violations across different cities in the US between January 2016 and December 2022, despite the stringent airspace regulations, installed security architectures, and huge investments in counter unmanned aerial systems (CUAS), otherwise known as drone defence systems (DDS) [7] (See Figure 1). Also, in recent times, several cases of drone-related airstrikes have been reported, targeting key infrastructure in different countries. Specifically, 170 out of 300 coordinated airstrikes in the Middle East were carried out using drones [8]. Although most of these drones were intercepted before they reached their target destination (thanks to CUAS and anti-missile systems), the social apprehension caused by this misguided and abusive UAV usage cannot be fathomed. This is a pointer to an impending danger and a wide gap between innovation's smartness, security, and safety.

The need for smart and safe aerial mobility falls under the third out of the five (5) fundamentals of the sustainable development goals (SDG) as approved by the United Nations (UN); which is peace (SDGs 10, 16) [9]. SDGs 10 and 16 focus on fostering peaceful, just, and inclusive societies, free from fear and violence. Hence, malicious and unguided usage of UAVs portends a serious threat to the actualization of SDGs 10, 16. Therefore, the need to assess the sporadic serialization, systemic sophistication, and security dynamics of UAVs as a viable alternative for smart aerial mobility (SAM) is critical. Fundamentally, SAM is a typical UAV network that combines a space network, an aerial network, and a ground network to maintain optimized resource allocation, timing, positioning, and navigation [10]. A loophole in any of these networks affects the overall security, smartness, and safety of UAV networks. This connotes that security intelligence in SAM demands a cross-layer secure communication framework that considers both physical layer security and the upper layer traditional security techniques to minimize security breaches on UAV networks [11].

The term "security" refers to a wide range of procedures and policies used to safeguard UAV operations, data, and systems from different types of threats. These precautions guarantee that UAVs can carry out their intended tasks in a reliable, safe, and secure manner. It encompasses cybersecurity, physical security, data security, communication security, operational security, etc. On the other hand, safety comprises steps taken to reduce risks, prevent accidents, and respond to emergencies due to environmental changes, thereby ensuring trustworthy operations. According to [7], the convergence of cognitive, cybersecurity, and cataclysmic intelligence forms the tripartite pillars for evaluating the trustworthiness of a UAV position, navigation, and timing. Thus, to guarantee secure, smart, and safe aerial mobility of UAVs that interlock the SDGs, an upward review and evaluation of the intelligence frameworks governing the principles of its operation is necessary. These security and safety intelligence frameworks go beyond artificial intelligence (AI) models to other disruptive technologies and parameters used in validating the transparency, reliability, and trustworthiness of a UAS application.

Cognitive intelligence entails UAV perceptions and interactions with signals within the airspace. It transcends beyond UAV detection, localization, and neutralization using CUAS technologies to software-defined radio (SDR) for improved signal processing, integrated sensing, and communication. Also, it includes software-defined unmanned aerial vehicles that navigate the airspace with little or no external network connectivity to reach their destination. On the other hand, cyber-intelligence in UAV-based logistics focuses on associated frameworks to maintain data privacy, transparency, and trustworthiness in a secure UAV network edge service scenario. It comprises associated technologies such as an intrusion detection scheme (IDS), directed acyclic graph (DAG), blockchain technology (BTC), and zero trust architecture (ZTA). Data is premium in a mission-critical cyber-physical system because unreliable or manipulated data ultimately yields misguided feedback from the inference of cognitive models controlling the UAV decisions [12]. Finally, cataclysmic intelligence encompasses self-navigation schemes (SNS) that enable UAVs to engage in simultaneous localization and mapping (SLAM) to interact with their immediate environment through associated sensors (visual, radio) and mediated learning to navigate their way to the desired destination with efficient collision avoidance mechanisms. Thus, when the UAV network fails due to a security breach, and a UAV in flight loses connection with the space, aerial, and ground networks, how does it maintain smartness and guarantee safety in operation without constituting a threat?

Several reviews and surveys have made consistent efforts to appraise technological developments in smart aerial mobility, as shown in Table 1. These works are inextricably linked to the significant proliferation and sporadic deployment of UAVs across domains. Only a handful of research works as well as technical reports from the National Aeronautics and Space Administration (NASA) have looked in this direction [13]. However, to the best of our knowledge, none of these works

TABLE 1 Summary of compared related works on smart aerial mobility developments.

Year	Reference	Database	Review Target area	Review Remark	Systematic Review	SLAM	Scope		
							XAI	BTC	ZTA
2020	[14]	×	UAV Comm. and networking	Mobility optimization	×	×	×	×	×
2020	[15]	×	Emerging drone services	Handling & ownership	×	×	×	×	×
2020	[16]	×	BTC-UAV network softwarization	SDN & NFV	✓	×	×	✓	×
2020	[17]	✓	BTC solutions for UAVs	Trusted computing	✓	×	×	✓	×
2020	[18]	×	UAV threat & vulnerabilities	Multi-factor authentication	×	×	×	×	×
2021	[6]	×	Drone-based package delivery	Use case and applications	×	×	×	×	×
2021	[19]	×	UAV in logistics	Path planning	×	✓	×	×	×
2021	[20]	×	Evolution of UAV	Internet of drones issues	×	×	×	×	×
2022	[21]	×	Smart logistics	Theories & applications	×	×	×	×	×
2022	[21]	✓	UAV applications in logistics	Path planning and routing	✓	✓	×	×	×
2022	[22]	✓	SDR-based solutions for safe UAV	CUAS techniques	✓	×	×	×	×
2022	[22]	✓	Software-defined radio systems	Antenna propagation & control	✓	×	×	×	×
2022	[23]	✓	Surveillance & smart city security	IoT, Edge, & C-ITS integration	✓	×	×	×	×
2023	[24]	×	Urban air mobility	Mechanism & challenges	×	×	×	×	×
2023	[25]	×	Security in UAVs & FANETs	UAV cyber-attacks	✓	×	×	×	×
2023	[7]	×	Drone transportation system	Mobility intelligence & security	✓	×	✓	✓	×
2024	[26]	×	XAI for Industry 5.0	Architectures & directions	×	×	✓	×	×
2024	[27]	×	Explainable AI for safe UAV	AI algorithms for safe UAV	×	×	✓	×	×
2024	[28]	×	IDS in autonomous Ethernet networks	Techniques and AI algorithms	×	×	×	×	×
2024	[29]	×	ZTA for UAV security systems	ZTA in military security	×	×	×	×	✓
2024	Ours	✓	UAV for smart & safe logistics	Security & safety intelligence	✓	✓	✓	✓	✓

has been able to address both the security and safety concerns of UAV operations in light of recent security threats (through advanced innovations) such as infoswarm. Also, with the rising introduction, popularity, and acceptability of SMiLE across the globe, it is critical to closely evaluate the safety and security implications of this eco-friendly innovation and provide empirical-based direction to issues that demand careful attention and consideration to meet the SDG pillars.

Therefore, this review is motivated by the need to provide insights into the security, smartness, and safety dereliction and developments in aerial mobility, with an emphasis on UAVs, by examining the cognitive, cyberspace, and cataclysmic intelligence that governs their positioning, navigation, and timing (PNT), especially as it relates to logistics. The specific contributions of the review are:

- We present an overview of smart mobility and intelligent logistics ecosystems and examine the disruptive tendencies and issues associated with using UAVs to extend SMiLE capacity based on empirical findings.
- We analyse the dynamics of the intelligence frameworks for ascertaining the smartness, security, and safety of UAVs in SMiLE.
- Next, we navigate the spectrum of cyber-cognitive attacks on UAVs and assay the security architectures to curtail them with the requirements for their adoption.
- Then, we highlighted the technological challenges and requirements for the adoption of security measures to improve the safety of UAVs, and finally, we provided research directions for the sustainable use of UAVs to expand the capacity of SMiLE.

Section 3 provides succinct evidence of SMiLE violations. Section 4 examines the dynamics in cognitive intelligence technologies. Section 5 traverses the cyber intelligence frameworks for data trustworthiness; Section 6 evaluates cataclysmic intelligence schemes that go beyond traditional UAV networks; and Section 7 relishes on open issues and future research directions for safe and secured SMiLE. The list of all acronyms used in this review article can be found in Table 2.

2 | REVIEW METHODOLOGY

This review adopts a combination of preferred reporting items for systematic reviews and meta-analyses (PRISMA) and sample population, phenomenon of interest, design of study, evaluation, research type (SPIDER) methodological approach to assessing and validating the intelligence frameworks that parameterize the smartness, security, and safety of UAVs in SMiLE. This is to ensure exhaustive paper selection sensitivity and specificity. Furthermore, snowballing was used to include grey

TABLE 2 Specific meaning of acronyms.

Acronym	Meaning
AI	Artificial intelligence
BTC	Blockchain technology
CUAS	Counter unmanned aerial system
DL	Deep learning
EAI	Edge artificial intelligence
FAA	Federal Airport Administration
GCS	Ground control station
GPS	Global positioning system
IDS	Intrusion detection system
IoD	Internet of Drones
IoT	Internet of Things
ML	Machine learning
PICOS	Participants, interventions, comparators, outcomes, and study design/limitations
PNT	Positioning, navigation and timing
PRISMA	Preferred reporting items for systematic Reviews and meta-analyses
SAM	Smart aerial mobility
SDG	Sustainable development goal
SDR	Software defined radio
SLAM	Simultaneous localization and mapping
SMiLE	Smart mobility and intelligent logistic ecosystem
SNS	Self navigation scheme
SPIDER	Sample population, phenomenon of interest, Design of study, evaluation, research type
UAS	Unmanned aerial systems
UAV	Unmanned aerial vehicles
V2I	Vehicle to infrastructure
V2V	Vehicle to vehicle communication
XAI	Explainable artificial intelligence
ZTA	Zero trust architecture

articles and online reports. The evaluation results are summarized and presented in tables using participants, interventions, comparators, outcomes, and study design/limitations (PICOS) metrics and charts for straightforward deductions and conclusions from the meta-analysis. Thereafter, the outcomes and prospects of each review objective section are discussed to reinforce the comprehension of the encapsulated findings.

2.1 | Research type

Review articles related to UAV security and safety for logistics were considered for qualitative evaluation (QE). Also, insightful information was extracted from the quantitative analysis (QA) of the data presented in technical papers to address the research questions and review objectives. Furthermore, case studies and online reports with evidence-based information for the advancement of security and safety in UAV mobility and logistics were also considered, as summarized by the statistics in Table 3.

TABLE 3 Review statistics.

S. No.	Database	QA	QE
1.	IEEE	72	6
2.	Wiley & Sons	4	*
3.	IGI Global	2	*
4.	Elsevier	19	5
5.	Springer	12	2
6.	MDPI	21	2
7.	ACM	1	*
8.	Others (arXiv, Taylor etc.)	27	5
9.	Online reports	12	*
	Total	157	20

In all, 8 digital libraries (see Table 3) were searched, namely IEEE, MDPI, Springer, Wiley & Sons, etc., and others (arXiv, Taylor, and other journals on Google Scholar) comprising 20 articles for QE and 145 technical papers for QA. At the same time, 12 online reports were accessed using snowballing. The phenomenon of interest used for exhaustive search of repositories includes keywords such as "unmanned aerial vehicle" and "logistics", or "unmanned aerial vehicle" and "security" and "logistics", or "unmanned aerial vehicle" and "safety" and "logistics", "unmanned aerial vehicle" and "security" and "logistics" and "explainable AI", or "unmanned aerial vehicle" and "safety" and "logistics" and "explainable AI", or "unmanned aerial vehicle" and "security" and "logistics" and "blockchain" etc. These keywords were chosen to reflect the PICOS strategy to address the research questions and meet the review scope and objective, as well as give room for article selection heterogeneity. The design of study used in this review for article gathering, screening, and eventual inclusion is summarized by Figure 2. After the preliminary screening of identified articles, duplicates were excluded. Thereafter, each article was screened for relevance, and eligibility criteria were applied to determine its inclusion or otherwise based on a full-text assessment. The evaluation and research type for the article's inclusion, exclusion, and eligibility criteria are summarized as; (i) the article is published in reputable journals and conference proceedings, (ii) the article is published in the English language, (iii) the article's publication year is 7 years (2017–2024), and (iv) the article's title and content cover the stated review scope and objectives.

3 | CONTEMPORARY DISRUPTIONS IN AERIAL LOGISTICS ECOSYSTEM

The advent of UAVs for logistics started in mid-2010. However, its popularity as a preferred alternative for priority logistics

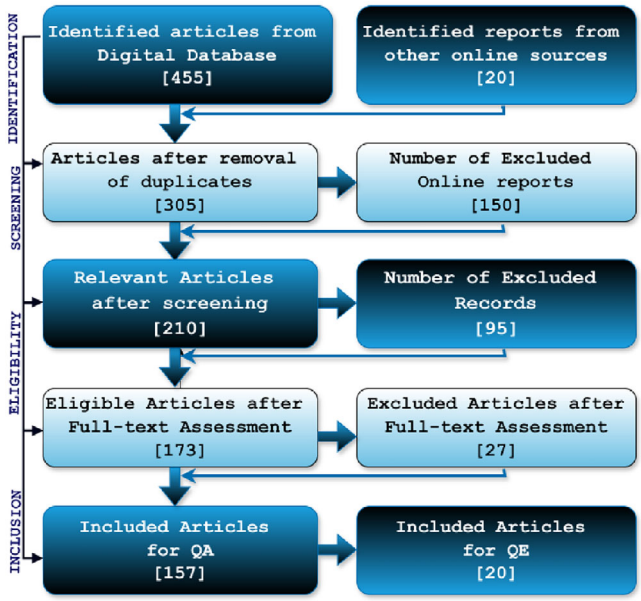

FIGURE 2 The PRISMA/SPIDER strategy for article gathering, screening, eligibility, and inclusion.

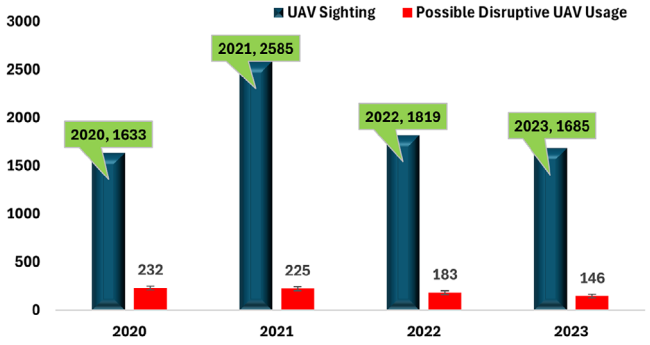

FIGURE 3 Side-by-side comparison of Genuine UAV usage and possible disruptive usage.

was fostered by Amazon in 2013 to deliver packages to its customers in mega cities within 30 min [30]. From 2016 to date, several logistics companies (such as DHL, UPS, JD.com, etc.) embraced UAV as a first-choice priority logistic delivery innovation due to advancements in UAV technologies such as increased payload capacities, safety features, longer flight times, etc. amidst attendant regulatory and risk issues. According to [21], UAV applications in logistics are classified into regional UAV transportation, and UAV express delivery (terminal distribution), UAV rescue (emergency logistics), and UAV storage management (inventory, inspection, etc.), with regional UAV transportation and UAV terminal distribution being the main forms. The deployment of UAV as an SMiLE solution aims to create seamless and efficient aerial transportation and logistics networks that leverage data and technology to address challenges such as congestion, pollution, and inefficient resource utilization caused by traditional air, rail, land, and sea logistics. UAVs enable real-time monitoring, decision-making, and optimized delivery, leading to more sustainable and resilient transportation and logistics systems. However, these benefits also introduce several disruptions to traditional air transportation globally.

For instance, UAV sightings recorded by the FAA [31] in different cities in the United States between 2020–2024 are presented in Table 4 showing the quarterly deployment of UAVs for different purposes across cities.

Between 2020–2024, a total of 8084 UAVs were sighted. The findings from Table 4 reveal a consistent pattern in UAV usage for smart aerial mobility, with peak usage being the second quarter (April–June) across the year under review (2020–2024). Also, 2021–2022 witnessed a surge in UAV usage, with a gradual decrease to 1685 in 2023. Consequently, the disruptive tendencies of UAVs in the logistics and air traffic ecosystem increased by 10.2% (823), as summarized by Figure 3. This disruptive usage includes UAVs that are not reported by the low earth orbit (LEO) satellite and UAVs that are not notified by the FAA. Similar to authorized UAV usage, possible disruption of the ecosystem by UAV peaked in the second quarter (April–June) between 2020 and 2023, with the year 2021 witnessing the highest value of 225 possible violations (see Table 4).

The findings from Figure 3 reveal that apart from 2020, with the highest UAV disruption of 14.2%, other years maintained an average UAV disruption of 10%. However, the first quarter report for 2024 indicates an 11.3% UAV disruption despite the advancement in security and AI techniques and technologies. These findings suggest that 10% security and safety risk is invariably too high a cost to be neglected if the sustainable usage of UAV in SMiLE is to be achieved. Furthermore, it doubts the veracity, reliability, and capacity of the existing underlying security architectures. Thus, an overhauling of these architectures becomes critical.

Several literature findings indicate a plethora of security and safety concerns associated with the usage of UAVs in SMiLE [20]. Security issues associated with drone deployment for logistics include airspace security, cybersecurity, payload security, and data privacy. On the other hand, safety issues include physical safety hazards, environmental impact, and interference with critical infrastructure (see Table 5). A breakdown of each of these issues is presented forthwith.

According to [7], each of these issues is a subset of the general drone-related concerns, which are categorized as drone user intention tracking, drone user-identity theft management, drone communication hijacking, drone user authentication, package delivery verification, and dynamic situation-aware drone engagement for minimal environment impact. Other safety-security issues of concern in smart aerial mobility for logistics include aerial transportation of unknown payloads, adaptive path tracking for quadrotors, adaptive anti-swing control for clasping operations in quadrotors with cable-suspended payload etc. Infoswarm (drone swarm for information warfare) is an emerging and multifaceted UAV deployment issue that involves the use of swarms of UAVs also known as the internet of drones (IoD) to create electronic, cyber, space, and/or psychological warfare [36] for competitive advantage, which can be offensive or defensive. Infoswarm leverages UAV swarm

TABLE 4 2020-2024 FAA report on UAV sightings and possible disruptive usage.

	UAV sightings					Possible disruptive UAV usage				
Year	**Jan–Mar**	**Apr–Jun**	**Jul–Sep**	**Oct–Dec**	**Total**	**Jan–Mar**	**Apr–Jun**	**Jul–Sep**	**Oct–Dec**	**Total**
2020	373	408	486	366	**1633**	59	71	62	40	**232**
2021	456	957	689	483	**2585**	49	66	66	44	**225**
2022	428	622	491	278	**1819**	44	69	51	19	**183**
2023	311	598	439	337	**1685**	27	50	37	32	**146**
2024	326	—	—	—	**326**	37	—	—	—	**37**
Total	**1894**	**2585**	**2105**	**1464**	**8048**	**216**	**256**	**216**	**135**	**823**

TABLE 5 Security and safety issues in UAV for logistics.

Security issues	**Indicators/specifics**
Airspace security	Collision avoidance [32], routing management [7], interference [24]
Cybersecurity	Network jamming, network hacking and code injection, code alteration, [33] exploitation of zero-day, exfiltration of data [34]
Data privacy	Spying, unlawful, and untracked intrusion,
Payload security	Identity theft, smuggling, risk of nuclear weapon carriage [13, 35]
Multifaceted	Infoswarm [36]
Safety issues	**Indicators/specifics**
Physical hazards	Inadvertent landing/crashes, drone-gun [37]
Environmental impact	Air pollution/fossil fuels, airspace
	Accidents [38]
Interference	Disruption of power lines, telcom. towers [39]

size, customization, and diversity, coupled with the integration of machine vision algorithms and the connectivity of devices for robust information management in creating swift vulnerabilities. This underscores that infoswarm cuts across cognitive, cybersecurity, and airspace security of UAVs as it affects not just the position, navigation, and timing information, but also targets the communication of UAVs, particularly the communication on the electromagnetic spectrum. Developing better cognitive models for effective spectrum management is key to addressing infoswarm. Also, the development and deployment of quantum communication for UAVs may likely reduce their dependence on the electromagnetic spectrum. This will certainly minimize the vulnerabilities associated with using UAVs for logistics and other purposes.

4 | COGNITIVE INTELLIGENCE FOR DYNAMIC UAV-SAFETY TASK PERFORMANCE

The rapidity of innovation in UAVs' underlying technologies makes intercepting and gorging these smaller aircraft a difficult task [39, 40]. The intelligence of AI models and associated technologies governing UAV PNT in the air influences their smartness and safety. While the sophistication and characterization of software-defined radios) and software-defined-unmanned aerial vehicles define aerial mobility smartness, CUAS dynamics help to address issues relating to their safety. Thus, analysing the developmental dynamics of these models and technologies will undoubtedly unravel the smartness and safety capacity of UAV usage in SMiLE.

UAVs operate on different frequencies. However, most commercial UAVs used for logistics operate in industrial, scientific, and medical (ISM) frequency bands of 433 MHz and 2.4/5.8 GHz. According to [7], CUAS approaches (otherwise called anti-drone systems or DDS) are cyber-cognito activities and techniques aimed at detecting (spotting an aerial object), identifying (eliciting its status), and neutralizing (mediation feedback synapses) perceived and premeditated malicious UAV deployment to create security breaches such as disruption of communication, disorientation of operations, the decimation of key installations, and possibility of divulging sensitive information, in a swift and unsuspecting manner [41] in a smart city. To maintain trustworthy aerial smart mobility, digital transformations force UAVs and CUAS techniques to compete dynamically, developing innovations aimed at outwitting each other's security intelligence and operational efficiency [37]. To ensure safety, CUAS models carry out three (3) main activities on UAVs; detection, identification, and neutralization (DIN), as depicted in Figure 4. For each of these activities, the underlying AI models carry out specific operations whose result is a determinant for triggering other activities. Various atmospheric and weather conditions, such as rain, snow, fog, dust, changing sunlight intensity, etc. significantly impact UAV smart mobility and, by extension, the functional capacity of CUAS for monitoring UAV safety [43, 44].

The possibility of simultaneous detection, identification, and neutralization of several drones is a more challenging task for most AI models in CUAS [7, 41] given different dynamic threat statuses. While few authors have attempted only multiple UAV detection and identification [37, 45, 46], the possibility of multiple neutralization of suspicious UAVs remains a doubt. [47] proposed the use of electromagnetic pulse (EMP) to achieve this feat. RF jamming performed using antenna arrays could also generate, utilizing signal processing methods (beamforming), multiple beams that could be targeted toward multiple

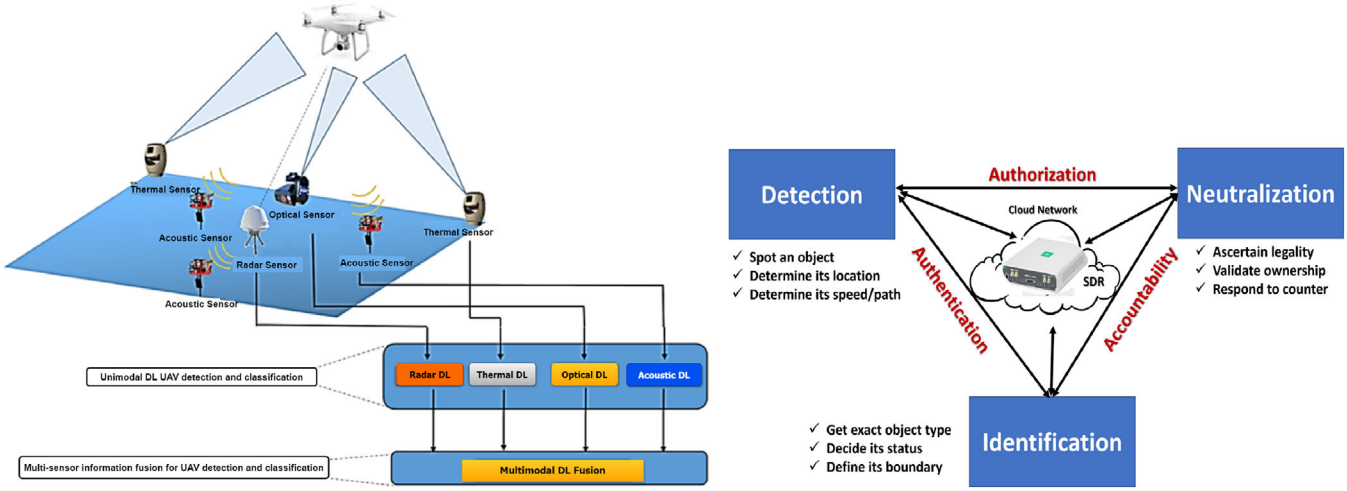

FIGURE 4 Highlights of UAV cognitive intelligence technologies (i) CUAS techniques for achieving smart and safe DIN operations [42]. (ii) Role of SDR in aiding authorization, authentication, and accountability of UAV.

target drones. However, the lack of legislation [7] on as well as stern restrictions by the Federal Communication Commission (FCC) on the manufacturing and use of RF jammers by private entities in an attempt to minimize abusive usage inadvertently slows the developmental pace of CUAS [22, 42, 48]. Furthermore, [7] hinted that accurate detection and proper identification of the status of payloads airlifted by UAVs by AI-empowered models remains a security issue. This is because the potential threat posed by a UAV used for logistics is not just the function of the failure of the UAV but also the harmfulness or otherwise of the attached payload [39]. Hence, AI models in CUAS should not only have the capacity to detect a logistics UAV and its payload but also provide details of the unknown object to avoid suspicion and unnecessary apprehension [37]. This increased transparency, however, comes with legislative and policy bottlenecks such as the protection of privacy and rights of the freight operator and the owner of the package delivery.

Also, situation-awareness response strategies are critical to distinguishing harmless and authorized logistic-based UAVs from malicious ones. For instance, the tactical intelligence for timely interception of a hijacked logistics-based UAV [49] is quite different from a disruptive logistic-based UAV to minimize disruption and fatality [50]. Also, proper identification and verification of package delivery by a UAV while maintaining user privacy by the CUAS pose cognitive puzzles. Drone-based sniffing techniques (though nascent) are a worthy attempt in this direction but with several limitations [51, 52]. As seen in Figure 4, CUAS cognitive intelligence models adopts hybrid (fusion-based) AI technologies and techniques in attempt to achieve smart and intelligent logistics through robust UAV threat analysis [37, 46, 53, 54]. However, the proposed AI models in these works are theoretical with little practical benefit.

An increase in UAV deployment ubiquity translates to increased exposure to security, and safety risks. According to [39], the danger of a UAV in the air is more of a function of the attached object or package delivery than the UAV itself. Since most UAV security threats are centred on the UAV networks, software defined radios (SDR) are deployed to improve UAV digital communication from code injections, spoofing, exploitation, etc. [55]. Also, most RF-based CUAS use SDR platforms to monitor and curtail UAV mobility for enhanced security and safety [22]. Initially, SDRs were designed to improve the interoperability between different communication systems of the US armed forces and ease corresponding logistics [56]. However, with the promise to minimize hardware dependencies (thereby leading to maximization of reconfiguration), their civilian application witnessed a surge. Thus, SDR serves as an intelligent agent to eliminate the need for specialized hardware by introducing software modules that implement as many communication functions as possible.

The objective function of SDR is to use the same simple and standardized hardware setup for multiple and different radio applications, where most of the signal processing is performed by software controlled by an AI algorithm. This ensures that the software code is as close to the antenna as possible, such that the signal processing of simple and standardized hardware setups for multiple different radio applications can be performed by the AI-enabled software. With the advent of 5G networks, SDR became part of the broader softwarization endeavour to adapt to 5G network designs and deployment. Softwarization aims to improve the flexibility of networks so that they can support a wide range of services. Thus, SDR offers cost-effectiveness, quality of service (QoS), flexible deployment and interoperability, adaptability, programmability, scalability, and wider frequency coverage [22], amongst other advantages.

To meet these mission-critical objectives in UAVs, SDRs are deployed in UAVs with AI algorithms as their underlying cognitive engines to enhance communication connectivity, increase channel characterization, improve security, and guarantee more accurate UAV detection, classification, and localization operation [57]. Figure 5 depicts a flight intelligent platform

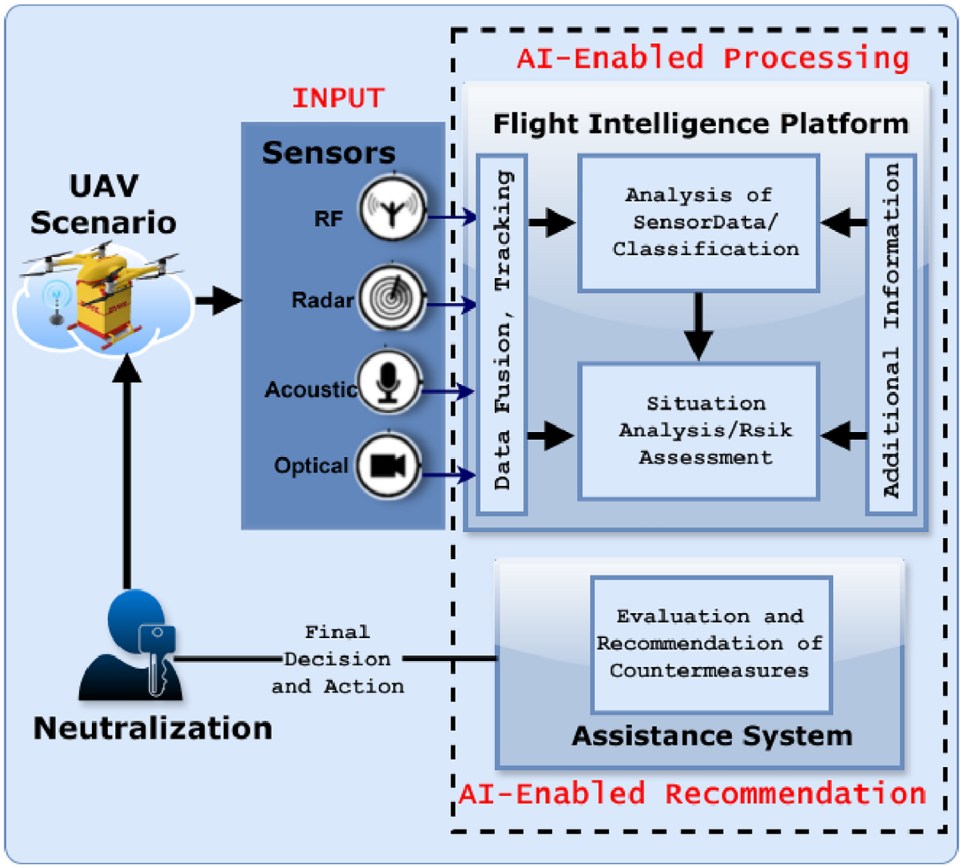

FIGURE 5 An ML-enabled multi-sensor SDR platform highlighting the hardware and software components for safe and secure UAV mobility.

highlighting the hardware and software components of an ML-enabled multi-sensor SDR for safe and secure UAS mobility.

SDRs facilitate efficient communication in UAVs by helping them mitigate channel impairments and adapt to changing environmental dynamics necessary during logistics operations. Also, with the ML-signal processing ability, SDR technology can implement advanced techniques such as signal enhancement algorithms, adaptive beamforming, noise cancellation etc. to improve signal quality and coverage. Furthermore, to improve security, SDR enables UAVs to adapt to their communication protocols and encryption methods in response to environmental threats.

To guarantee public safety and UAV intelligence surveillance, and reconnaissance, the hardware and software design of an ML-enabled multi-sensor-SDR incorporates different wireless technologies such as cognitive radios (CR), frequency hopping spread spectrum (FHSS), and mesh networking. This provides self-healing networks to UAVs to enhance situation analysis and environment-awareness navigation, as well as improves the scenario-specific and dynamic neutralization capacity of CUAS systems. This aids in guarding against the malicious deployment of UAVs to disrupt aerial autonomous vehicular mobility that endangers the sustainability of UAS applications. While CR allows for efficient allocation of unused frequency channels, resulting in improved quality of service, reduced interference, and increased spectrum efficiency, FHSS uses randomized frequency changes several times a second to protect critical data.

Cognitive intelligence (such as GNU radio signal analysis, processing, and prediction) in SDR platforms are carried out using different input parameters and algorithms such as multiple signal classification (MUSIC) [58], Raytheon Associative/Array Processor (RAP) [58], received signal strength (RSS) [59], RF jamming [60, 61] etc. with attendant limitations. To overcome the inherent limitations in these methods, ML-enabled SDRs are proposed by different authors, as highlighted in Table 6.

Nie et al. [62] combined different ML classifiers to achieve a multidimensional signal feature indication, which was deployed on a USRP X310 SDR platform for drone detection and identification. However, the detection range was short. Likewise, the AI model proposed by [63] achieved 99% accuracy, but the signal strength would be less ideal in the real detection process, in which the signal strength declines on an exponential scale. The better signal feature extraction method has to be investigated for high accuracy of detection when the controller signal is less strong than the wireless signal noise. [66] combined four RF classifiers to detect four types of jamming signals in UAVs. Though the detection rate was high, it was marred by several mispredictions as environmental changes increased. [62] capitalized on the signals between the UAVs and the ground controller and successfully discriminated between non-UAV

TABLE 6 Proposed ML-enabled SDR for safe UAV mobility.

Author	AI model-technology	Scope of UAV monitoring	SDR outcome & limitations
2021 [62]	RF, SVM, KNN, RF-based	UAV detection	Achieved 3D positioning accuracy of 2.35m and a detection accuracy of 95.58%. Not tested in a real environment.
2021 [63]	KNN RF-finger printing	UAV detection	99.9% detection accuracy with 5 UAVs and accuracy reduces as the number of UAVs increases. Only effective in near-field scenarios and unsuitable far-field regions due to signal noise/interference.
2021 [64]	KNN, XGBoost RF-finger printing	UAV detection & identification	99% D & I accuracy. Simulation-based and limited to only 2 UAV models. Only close-range detection
2021 [65]	DRNN RF-based	UAV detection	99% UAV classification accuracy. Only 9 UAV models are used. Simulation-based.
2022 [66]	Ensemble RF	UAV jamming detection	Only 4 jamming types covered. The detection rate was 93% with high mis-predictions in different scenarios.
2022 [62]	SVM, RF, and KNN using RF signals	UAV detection and positioning	Can detect only DJI Spark using Ettus USRP X310.
2024 [67]	Deep CNN and LR using RF signals	Imagery UAV detection	Detect 3 types of UAVs using NI USRP 2943 SDR.
2024 [68]	CNN RF-signal capturing	UAV classification, TDOA-based positioning	Cost-effective classification of 4 UAV types at different domains.
2022 [22]	3EED algorithm using RF signals	UAV detection and defence	Localization of 4 UAVs by estimating their AoA.
2024 [69]	Path-loss and PRACH method	UAV localization	Ground transmitter localization of Tarot X6 hexacopter based on RSSI and AoA estimation.
2024 [70]	MUSIC algorithm using RF signals	UAV localization	Guarantee safety drone positioning and pinpointing based on RF signals by NI USRP 2954R SDR. Limited to DJI Mavic 3T Basic Enterprise.

and UAV signals despite increased environmental noise and interference. The system combined advanced signal processing techniques such as empirical mode decomposition (EMD), STFT, and Fourier transformation to detect and position UAVs. Finally, [68] deployed the CNN algorithm on Ettus USRP X310 to capture RF signals of Parrot Bebop, DJI Phantom, Fimi, and DJI Mavic UAVs. The system achieved high UAV detection and localization at different domains and TDOA-based positioning. Besides the use of AI algorithms to boost the performance of SDRs for UAV accurate detection and positioning, authors deployed different techniques in SDRs. [22] deployed 3EED algorithm in Ettus USRP X310 to detect and localize four DJI models based on AoA estimation. Likewise, [69] deployed path loss and PRACH algorithm on ADALM-PLUTO to localize Tarot X6 hexacopter via RSSI and AoA estimation. Finally, [70] deployed the MUSIC algorithm on NI USRP 2954R to address safety concerns in DJI Mavic 3T Basic Enterprise by ensuring accurate pinpointing of its position.

The findings from Table 6 indicate that most AI models in SDR designs are only RF-based, limited to detection, and have implicit AI algorithms, which are ineffective for scenario-specific and safe UAS operation. Understandably, an important limitation of RF-based CUAS is related to the impossibility of detecting and annihilating autonomous drones in cases where they have a predefined flying path and do not have any active data communication with an operator located on the ground. This implies that most of these cognitive models are yet to address other fundamental issues in UAV for SMiLE, such as package delivery authentication, verification, and validation, which are critical for curtailing smuggling and the transportation of illegal and dangerous substances via UAV. Drone-based sniffing detection is gradually gaining traction in the detection of explosives, nuclear weapons, and hazardous materials being transported across borders and in congested areas [51, 52, 71]. However, it is still nascent and demands more research effort, as the development of more UAV-based sniffing techniques and models will greatly improve UAV operations in SMiLE. Also, there is a need to investigate combined RF signal detection, localization, and classification using the latest computer vision methods and compare their performance with the two-stage detection and classification methods. Finally, as seen in Table 6, SDR cognitive models are yet to integrate concepts such as explainable AI (XAI), federated learning (FL), self-supervised learning (SSL), edge AI (EAI) etc. for optimal performance in accelerating safety deployment of UAVs.

Nowadays, SDR is designed with the mesh capacity for the self-healing network (SHN) or self-forming network (SFN) to enable long-range and self-navigating strategies (SNS) in UAVs thereby enhancing the safety deployment of UAV intelligence for logistics, surveillance, and reconnaissance. Common examples of SDRs produced by RDTech [72] with cutting-edge software, SHN with multiple nodes capacity, and improved throughput via unlimited hops include RDL-2 (100 km), RDL-3 (200 km), RD-SR/MR/LR/XLR (omnidirectional signal

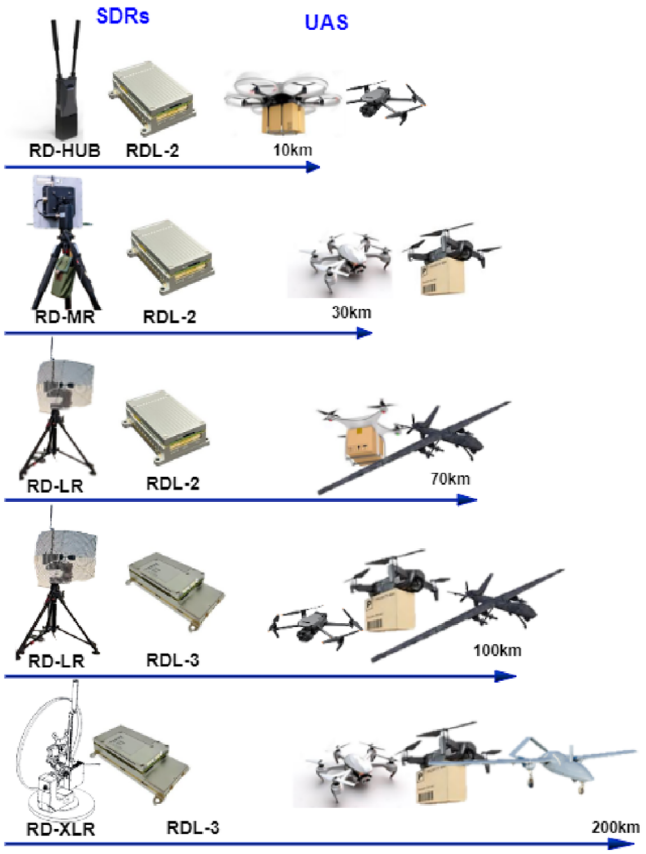

FIGURE 6 Typical SDRs with cutting-edge software and self-healing network capacity for long-range UAS navigation.

tracking with ranges of 15, 30, 100, and 200 km), RD-HUB (10 km), RD-MR(30 km), RD-LR, RD-L-2 (70 km), RD-LR, RDL-3 (100 km), RD-XLR, RDL-3 (200 km), RD-Edge (see Figure 6). For instance, the RD-HUB has a mission-critical wireless networking hub capacity of up to 32 nodes, allows SHN, and provides a throughput of 20 to 40 Mbits. This increase in the long-range navigation capacity of SDRs attests to the developmental improvements of the abilities of their underlying cognitive models and associated technologies for efficient signal capturing and processing.

The smartness and safety of UAV cognitive intelligence depend largely on the explainability of the AI model that controls its operation. Achieving a trade-off between security, speed, and scalability in mission-critical and time-sensitive cyber-physical systems (CPS) by incorporating secured XAI remains a daunting challenge for safe UAS applications.

5 | CYBER-RESILIENCE IN UAV LOGISTICS NETWORKS: TAXONOMY OF ATTACK & SMART ARCHITECTURES

UAVs' network topology dynamics differ from those of vehicular ad hoc networks (VANETs) and mobile ad hoc networks (MANETs). Typically, UAVs use the flying ad hoc network (FANET), which is a subset of MANETs. In addition to single-UAV operations, cooperative and connected intelligence communication in UAVs (UAV-to-UAV), which is enabled by FANETs, is becoming common in many UAV applications, especially in SMiLE. However, FANETs stand out from other ad hoc network types due to their unique features in response to the high mobility of UAVs. One of the most distinguishing features of UAVs' FANET is their ever-evolving topology, which allows the building of a high-speed (above 720 km/h) and extensive communication ecosystem (terrestrial, aerial, and space networks), thereby promoting an innovation known as drone transportation system [7, 37]. Consequently, this exposes UAVs' FANET to high vulnerabilities and constant cyber-cognitive attacks of all shades and forms due to their reliance on wireless communication and distributed control systems.

Generally, cyber-attacks on UAVs' FANET are categorized as either physical or logical attacks, based on their distinct characteristics, such as cracking or jamming, exploitative, infectious, information-gathering, interceptive attacks etc. [7, 73]. Attacks on UAV networks can be either active attacks or passive attacks, depending on the intention of the intruder on the communication network. However, a broader categorization of UAV attacks can be established based on the vulnerabilities associated with FANETs, as an integral part of the ground base station. According to [25], the taxonomy of surface analysis of attacks on UAVs can be grouped into three (3): UAV-component attack, UAV-communication layer attack, and UAV-communication architecture attack. Table 7 presents details of broad categories of cyber-attacks specific to UAV deployment and their overall impact in SMiLE.

Firstly, UAV-component attacks are targeted at the hardware, sensor, and software components of the UAV. Hardware-based attacks include supply chain attacks, battery attacks, and side-channel attacks. Sensor-based attacks focus on manoeuvring the inherent weaknesses in the UAV sensors to disrupt its operations and this includes jamming attacks, GPS spoofing attacks etc. On the other hand, software-based attacks are targeted at the confidentiality, integrity, and availability (CIA) of UAV system components such as navigation systems, flight displays etc. Zero-day, malware, and backdoor attacks are some of the most common types of software-based attacks in UAV networks. Secondly, a UAV communication layer attack targets the physical, network, and transport layers of the UAV. The most common of these attacks are eavesdropping, jamming, and routing attacks. Finally, attacks on UAV-communication architecture target UAV-to-UAV and UAV-to-others (satellite, GCS etc.). Other forms of cyber-cognitive attacks on aerial networks and designs include phishing and social engineering, password attacks, data breaches, advanced persistent threats (APTs), insider threats, GPS spoofing and jamming, brute force attacks, firmware attacks, and physical tampering of the aerial and terrestrial infrastructure.

Ad hoc networks such as FANETs have advanced and unique characteristics of improved protocols for faster cooperativeness of nodes in the network in terms of packet delivery ratio (PDR) and energy efficiency [25, 74, 87]. However, the findings in Table 7 indicate that most of the cyber-attacks are still targeted at the routing protocols of UAVs and suggest a gap

TABLE 7 Spectrum and impact of cyber-attacks on UAV networks.

No.	Aspect of UAV	Targets	Sub-targets	Nomenclature of UAV cyber-attacks	Description and impact of attacks-vulnerabilities
1.	**UAV-communication layer**	Network layer (routing attack)	Traffic attacks	Greyhole (dropping)	The dropping attack involves an attacker selectively discarding received packets (greyhole), either dropping all of them or targeting specific packets intended for a particular destination. It is aimed at the wrong routing of aerial networks [74, 75]
				Sybil	It is an impersonation attack where attackers use the addresses of other nodes or fabricate addresses not present in the network to divert the UAV [76, 77].
			Topology attacks	Sinkhole	Attackers falsely claim to offer a more efficient route to a specific destination. If the source node falls for this deception and selects the advertised route, the attacker node can intercept and monitor all network communication between the source and destination nodes. It serves as an initial step before launching subsequent attacks like dropping and altering data packets [78, 79].
				Blackhole	The blackhole attack is a two-step method that combines sinkhole and dropping attacks. It disrupts communication and escalates energy consumption within the network thereby reducing network lifespan [80, 81].
				Wormhole	Wormhole attacks on UAVs are a specific kind of cybersecurity risk in which malicious parties build a wireless network wormhole (tunnel or shortcut) between two distant points in a wireless network [82, 83].
				Rushing	Rushing attack is a DOS attack that is capable of being effective against various reactive protocols used in ad hoc networks, including AODV, DSR, SAODV, and SUCV. Rushing attacks ignore MAC, create routing layer delays, fill additional transfer node queues etc. [25, 84]
				Network reconnaissance	Attackers scan and probe for holes in terrestrial security networks to find openings they can use to launch additional attacks. By inserting harmful Structured Query Language (SQL) statements into web apps or backend databases, to manipulate sensitive data without authorization [85]
		Physical layer	Resources attack	Replay	Replay attack (a subset of DOS attack) involves re-sending outdated yet valid data with the intent of impeding or halting communication. This attack causes a reduction in aerial network responsiveness [81, 86]
			Jamming attacks		Aims at disrupting UAV's communication and network communication by generating stronger signals than the UAV signal [34, 87, 88].
			Eavesdropping attacks		A passive attack that violates UAV network privacy to listen to communication without interrupting signal transmission [89, 90].
		Transport layer	UDP attack TCP attack	UDP flooding, SYN flooding, session hijacking	attacks target loopholes in transport layer protocols, user datagram (UDP), and the transmission control protocol (TCP) [84, 91, 92]
2.	**UAV-communication architecture**	U-2-U	Data tampering attacks		Attacks to manipulate UAV data that result in inaccuracies of vital information such as UAV navigation data, direction, position, and altitude [93].
			De-authentication		Deauth is a denial of service (DOS) attack that obstructs communication between routers and devices thereby making targeted users disconnect. It makes use of IEEE 802.11 wireless networks since they offer the necessary de-authentication frames [94, 95]
			Sybil		It is an impersonation attack where attackers use the address of other nodes or fabricate addresses not present in the network to divert the UAV [76, 77].
			Jamming attacks		It aims at disrupting the UAV radio signals by introducing pulses and noise. These days, Frequency Hopping Spread (FHSS) and Direct Sequence Spread Spectrum are the two methods for preventing jamming attacks [96, 97]

(Continues)

TABLE 7 (Continued)

No.	Aspect of UAV	Targets	Sub-targets	Nomenclature of UAV cyber-attacks	Description and impact of attacks-vulnerabilities
		U-2-others	Drone in the middle (DiTM)		In DitM, the attacker secretly modifies and sends the navigational messages that are sent and received between the drone and its connected navigational control system. This leads to session hijacking, DNS spoofing, and packet sniffing [98, 99]
			Spoofing attacks	Steppingstone assault	Targets a swarm/host of aerial networks by targeting the closest UAV with false data and the attack command is relayed by intermediate UAVs (hops) until it reaches the destination UAV nearest to the target system [100].
3.	**UAV-components**	Hardware-based	Battery attacks	Depletion of battery (DoB)	DoB target UAV charging systems as well as depletes battery power faster than the usual time by sending fake requests that lead to voltage fluctuations [101, 102].
				Denial of sleep (DoSp)	DoSp causes UAVs to use power continuously by preventing them from entering sleep mode [103].
			Hardware-Dos attacks		Denial of Service (DoS) attacks aimed at UAV hardware components by making it exhaust resources and cause the UAV to miss the delivery and arrival at the destination deadline [104–106].
			Supply chain attacks		Attacks that exploit the security loopholes that occur during UAV components procurement, such as using 3D design files to produce faulty UAV parts [107, 108]
			Side-Channel attacks		It exploits leaked information from tasks executed via microelectronic components. Authors [110] grouped side-channel attacks into electromagnetic radiation attacks[], power-consumption attacks, and time-based attacks [109]
		Software-based	Backdoor attacks		Attackers scan and probe for holes in terrestrial security networks to find openings they can use to launch additional attacks. By inserting harmful Structured Query Language (SQL) statements into web apps or backend databases, to manipulate sensitive data without authorization [110].
			Malware attacks		It force UAVs to navigate towards the attacker's specified locations to hijack the UAV control [78].
			Zero-day attacks		Attacks that are launched on UAV software due to delays by vendors to update patches [111, 112].
		Sensor-based	GPS spoofing attacks	Active GPS spoofing passive GPS Spoofing	Used to alter planned UAV behaviour and assume control of the device by introducing falsified data into the device [113, 114].
			Jamming attacks		Interruption of sensor signals to prevent the UAV from receiving valid sensor information [34, 87, 88].

in mechanisms and strategies for enhanced security across the layers of the UAV networks. Specifically, these routing protocol attacks on the UAV can cause it to depart from its intended flight route, display unpredictable behaviour, or even interrupt communication from the remote control, with an inestimable impact.

Overall, these attacks have a significant impact on the safety deployment and scalable technology diffusion of UAVs as a sustainable alternative for smart and intelligent logistics. [25] examined the impact of routing attacks targeted at the network layer of the UAV in both low-density networks and high-density networks using a 3D GMM mobility model to simulate the 3D natural flight of the UAVs. The routing attacks cut across attacks on topology (sinkhole and blackhole), attacks on traffic (dropping), and attacks on resources (flooding). The performance metrics used in evaluating the performance of the UAV networks with an increase in attack ratio are packet delivery ratio (PDR), end-to-end (E2E) latency, and overhead. The result of their findings is summarized in Figure 7.

From Figure 7, an increase in attackers ratio of flooding and sinkhole attacks led to a sharp decrease in packet delivery ratio (PDR) in both low-density and high-density UAV networks. Although PDR seems to remain unchanged for blackhole and dropping attacks with an increase in attackers ratio, the attack still changes the UAV network's behaviour with a significant indirect impact on the overall ecosystem. Unlike PDR, an increase in attackers ratio of sinkhole, dropping and flooding brought about a rise in the E2E latency of the UAV network due to the establishment of longer alternative routes, with the flooding attack having the highest impact in both low-density and

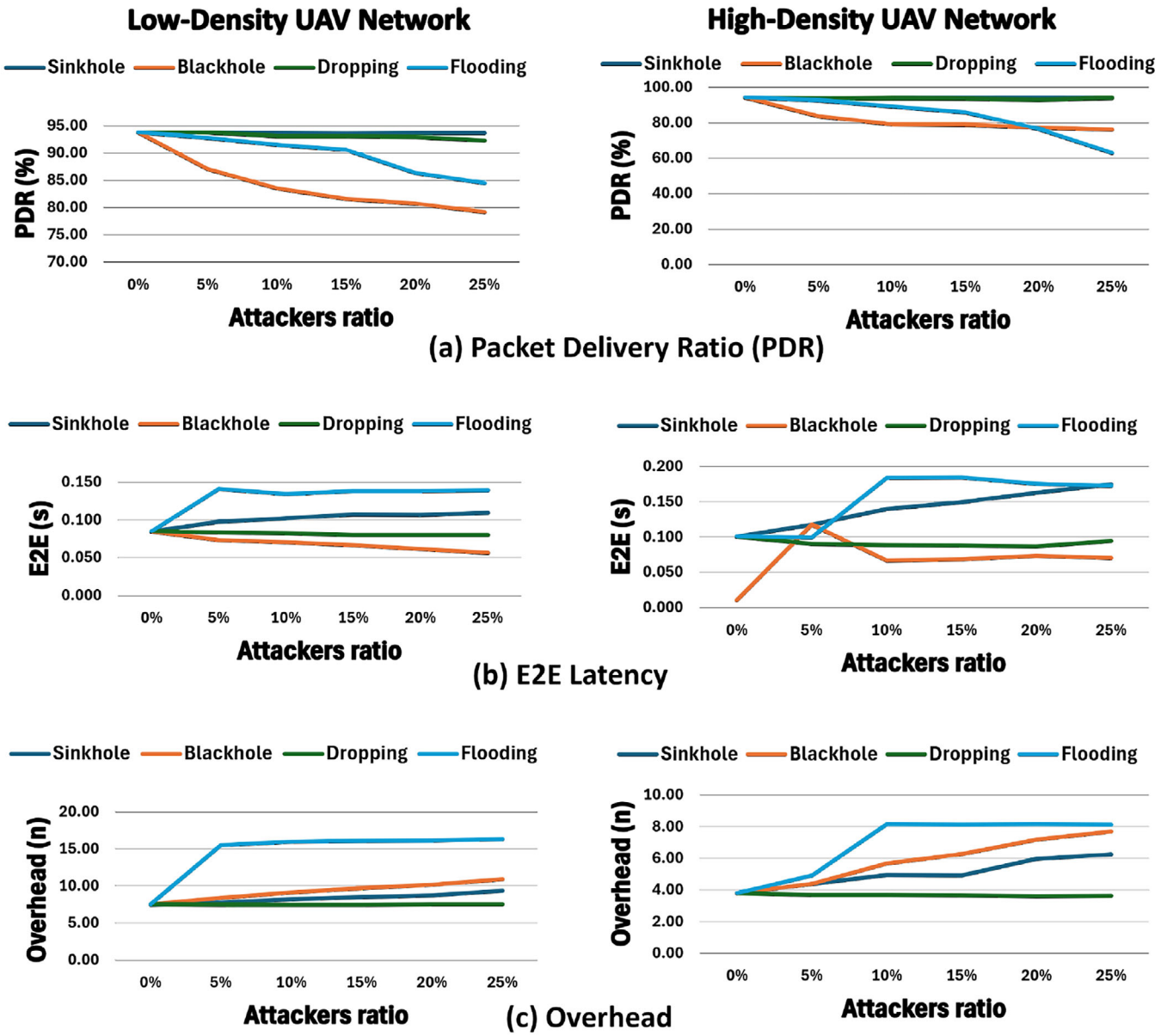

FIGURE 7 Impact of routing attacks on low-density and high-density UAV networks based on (a) packet delivery ratio (PDR), (b) E2E latency, and (c) overhead, with an increase in attack ratio.

high-density networks. However, as the number of blackhole attacks increased, E2E latency declined posing a serious threat to the reliability and safety of the FANET. Finally, UAV networks with high volumes of routing attacks resulted in increased overhead leading to depletion of vital resources and intensified network congestion. An increase in dropping attacks seems to exhibit minimal impact on the network overhead. However, the overall impact of dropping attacks (including PDR and E2E latency as discussed earlier) on the UAV network is not negligible in ascertaining safety deployment.

To maintain confidentiality, integrity, and availability in UAV networks and guarantee their safety, several cyber-cognitive and security architectures are designed to counter (prevent) and curtail (defend) the impact of cybersecurity attacks in FANETs. These security architectures are aimed at improving the network resilience of the IoD as an integral part of the Internet of Everything (IoE) to create an Internet of Value (IoV) ecosystem that is sustainable and reliable. Prevention techniques are highly effective against common and known attacks. However, with the emergence of insider and new attacks unknown to these architectures, they are likely to perform poorly. Prevention techniques are effective. Blockchain technology [115–117], authentication mechanisms [118], physical-layer security [119, 120], sensor-based methods [121, 122] etc. are common UAV cyber-attack prevention approaches. To complement prevention schemes, intrusion detection schemes (IDS), are widely deployed in UAV networks for cyber-attack detection [123, 124] to identify potential attacks before the system's CIA is

TABLE 8 AI models for cyber-intelligence in UAV networks.

Security approach	Method/AI model	Attack type (s)	Potentials& Limitations
Prevention	Key agreement [127]	Desynchronization, DiTM, Leakage, Impersonation, Offline Password Guessing	Blockchain-based to address anonymity.
	Authentication scheme [128]	Brute force, DoS, DiTM, Impersonation, Replay	No simulation were conducted. No dataset.
	Mutual authentication protocol [129]	Eavesdropping, DiTM	No dataset was mentioned for reproducibility.
Detection	FL [124]	GPS Spoofing, GPS jamming	No simulation
	FL [130]	GPS jamming	No simulation
	FL [131]	Jamming	No simulation
	DL [132]	Brute force, Botnet, Dos, port scanning, XSS	No implementation
	DL [133]	Backdoor, Dos, DiTM, injection, Password, Scanning.	No implementation
	ML [134]	Time delay	No dataset
	ML [135]	Sybil	System complexity
	ML [136]	GPS spoofing	No dataset
	ML [91]	DoS	No actual implementation
	ML [137]	DoS, DDoS, brute force, Botnet, web attack, infiltration	Limited application
	ML [138]	GPS spoofing	Limited application
	ML [139]	Blackhole, greyhole, GPS spoofing, GPS jJamming	System complexity
Hybrid	DL [73]	GPS spoofing, GPS jamming	No implementation was carried out

comprised. Recently, the need for a hybrid intrusion prevention scheme (IPS) rather than the typical IDS for UAV networks is gaining momentum [125, 126].

AI algorithms are utilized as the underlying inference engine of these security architectures for efficient cyber-attack and intrusion pattern discovery and analysis, enhance their cyber-resilience potentials, and guarantee optimal performance. This is due to the velocity, variability, and attack volumes emanating from multiple IoD nodes and devices. Typically, UAVs have resource-constraint hardware characteristics due to their compact nature. Hence, AI algorithms researchers propose to curtail cyberattacks are lightweight models with minimal computational complexity. This is to meet the energy consumption-conscious design of UAVs. Table 8 highlights adopted lightweight security measures and accompanied AI models for cyber-resilience in UAV networks.

The limitations of these suggested approaches and AI techniques imply that disruptive technologies' dynamic evolution has not yet fully caught up with the risky nature of cyberattacks directed towards them and the corresponding vulnerabilities these technologies produce. Hence, there is a need for ardent research efforts towards in-depth study of the characterizations of contemporary and emerging attacks. This will help to re-invent the wheels in developing perspicacious cognitive models that can counter and curtail dynamic attacks with optimal results. Thus, trustworthy, smart, and safe UAV deployment for logistics and other purposes requires a robust framework that can examine cyber-attacks at all layers of the UAV networks (communication, architecture, and components) and authenticate users through an AI-software-centric modular paradigm as shown in Figure 8.

The authorized defence control centre (usually state actors in charge of the CUAS) must have the capacity to handle multiple UAV cyber-attacks and intrusiveness at the cognitive, cyber, and physical layers of the UAV network with enhanced security authentication scheme for thorough UAV user or operator validation. The underlying software has to be driven by an AI-integrated application programming interface (API) to perform authentication, authorization, session handling, data protection, error handling, versioning, and service discovery, and input validation. Since most cyber-attacks on UAVs are targeted at distorting the signal parameters of operators, adopting a security intelligence that incorporates cross-layer security designs will undoubtedly enhance UAV-user authentication [11]. The authentication strategy should be robust to handle improper authentication issues, authentication bypass using an alternate path or channel, missing critical steps in authentication, key exchange without entity authentication, improper certificate validation, and improper checks for UAV-user certificate revocation. However, several studies have shown that the incorporation of blockchain technology and zero-trust architecture into UAV security intelligence can address all these authentication features and limitations of AI-empowered approaches (see Section 7).

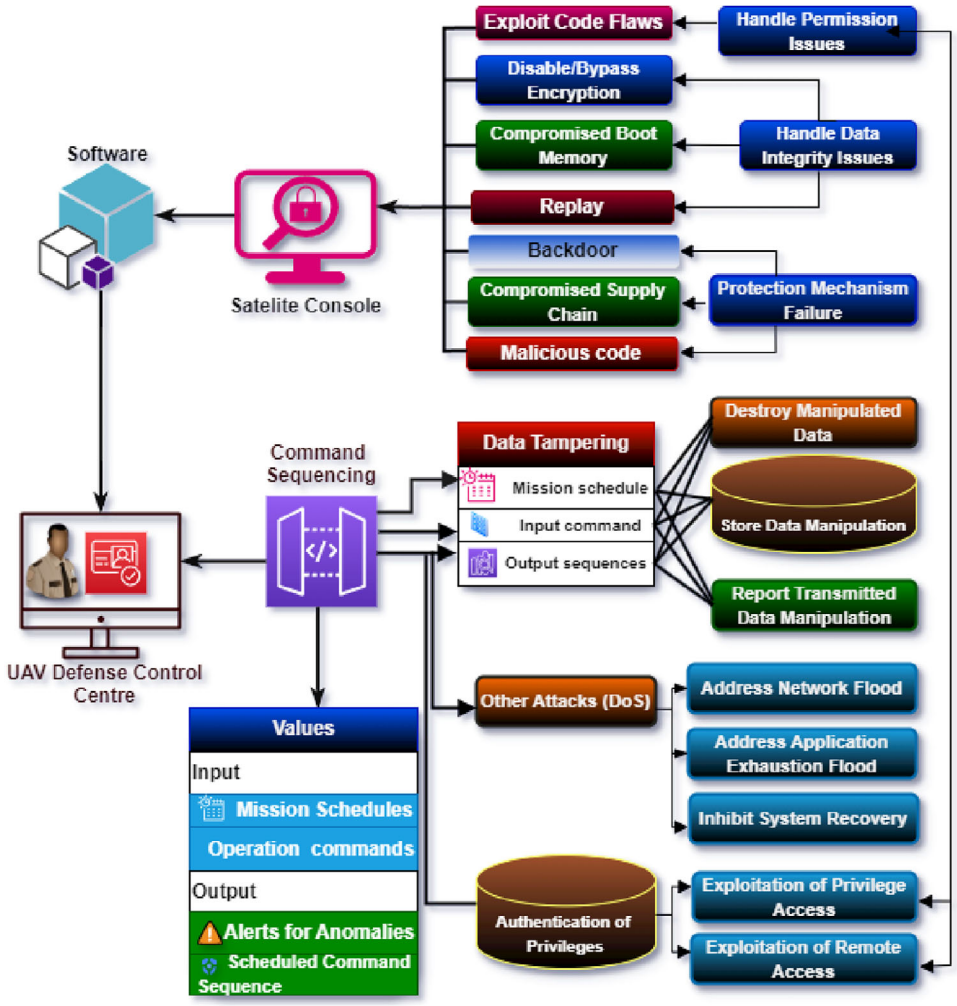

FIGURE 8 A software-centric AI-empowered cross-layer security architecture for resilient cyber-intelligence in UAV networks.

6 | DECISIVE SITUATIONAL AWARENESS IN UAV-BASED LOGISTICS

One of the physical security and safety concerns in aerial-based mobility and logistics is the intuitive and effective control, and stability of suspended payloads that are attached to UAVs and quadrotors from fallen off [140]. Due to uncertainties in the UAV operating environment (such as external wind, parametric, rotor downwash etc.), there is a high probability of a payload falling off a UAV, and the associated risk might be inestimable. Current techniques and technologies for ensuring the stability of suspended payloads to quadrotors lack the intuitive capacity to respond to sudden external changes. Thus, AI-empowered adaptive anti-swing controllers that incorporate state-dependent parameters and uncertainties in their design will aid in improving the stability of suspended payloads by logistic UAVs, especially quadrotors. This will help to capture uncertain clasping and unclasping operations of the suspended payload [140]. Beyond this, safe and secure autonomous navigation and landing of UAVs are essential parameters and functions for measuring their smartness and intelligence in an unknown environment, ensuring terrain safety, cognitive perception, and efficient path planning.

Models for motion control for autonomous vehicles cut across predictive control model, barrier functions/Lyapunov barrier functions, control barrier functions, and prescribed performance control [141, 142]. These approaches are for time-varying trajectories and are unsuitable for UAV logistics. Path-following control architectures with user-defined spatial path parameters are deployed to overcome these limitations [143]. Authors [141] proposed an environment-aware dynamic constraint path-following architecture for quadrotors that is resilient and adaptive to system uncertainties and unknown attackers. However, the architecture lacked experimental verification to validate its practical usefulness. Also, the uncertainties and noises associated with the sensors and actuators were not addressed.

Conventionally, UAVs perceive, interact, localize, and navigate their immediate environment through simultaneous localization and mapping (SLAM) using associated sensors and

network connectivity. The objective function of SLAM is the automation of the sensing and navigation system of an autonomous robot in an unknown environment [144]. Through the aid of SLAM algorithms, a UAV can reconstruct the map of its surroundings and localize itself in the map, which helps it explore and navigate regions that are challenging and inaccessible by humans. This is essential for logistic-based UAVs to maintain their defined path and adapt intuitively in response to sudden environmental dynamics while navigating to their target destination. Consequently, logistics-based UAVs relish these self-navigating strategies (SNS) to arrive at their destination via the implementation of associated sensor technologies for measurement acquisition based on captured data characteristics. However, current conventional SLAM methods in UAVs heavily rely on geometric maps and/or positioning devices, resulting in two (2) issues: (a) blockage of signals leads to UAV failure, and (b) inability of navigation systems to achieve high-level decision-making for advanced critical missions [145].

The two most commonly implemented SLAMs in UAVs are visual SLAM (VSLAM) and radio SLAM (RSLAM).VSLAM entails the use of camera sensors (monocular, stereo, and colour), while RSLAM uses electromagnetic waves (such as radio signal-based sensors, especially radio frequency identification (RFID)) to sense the environment. Other widely used technologies include ultra-wideband (UWB), light detection and ranging (LiDAR), ultrasonic, Bluetooth, and wireless fidelity (WiFi) [146]. Unlike VSLAM, which is faced with high storage costs and reusing the metric map issues, R-SLAM is best suited for privacy-sensitive applications. Cooperative SLAM, otherwise known as collaborative SLAM (CSLAM) [147–150], enables faster exploration and navigation of several autonomous robots through connected intelligence and semantic communication [145] for efficient information sharing. Each SLAM approach utilizes different cognitive algorithms to process sensor information and produce an outcome upon which the robots act with inherent issues.

These days, to increase the performance efficiency and effectiveness of SLAMs in UAVs, optimization algorithms and hybrid approaches (sensor fusion), which involve the combination of multiple sensor types (radio and visual), are adopted for multiple robot navigation. Some common examples are UWB and LiDAR [151], and camera and UWB [146], with inherent drawbacks such as geometrical irregularities, localization inaccuracies, and missed detection [152] etc. However, fusion algorithms usually impose additional system computational overhead [153], thereby constraining the real-time capability of SLAM in UAVs. Furthermore, to maximize area coverage and decrease mission latency, UAV systems are equipped with an onboard swarm-based CSLAM self-navigation strategy [148], thereby reducing swarm redundancy and improving the robust cooperativeness of groups of UAVs. Though the onboard CSLAM proposed by authors [148] is limited to ultra-constrained nano-UAVs with a defacto system technology, it paves the way for the development of advanced navigation solutions for increased safety in UAV flight autonomy through efficient path planning strategies. However, CSLAM technology in UAVs is constrained by limited accuracy and range. Also, it is highly sensitive to environmental conditions and is often faced with satellite denial scenarios, especially when the GNSS signals encounter interference, spoofing, fading, and multi-path effects. Table 9 presents recent collaborative SLAM strategies adopted in UAVs and the performance of the underlying cognitive models for enhancing the smartness and safety of UAV usage.

The few advanced navigation and path planning strategies presented in Table 9 are credence to the conscious research and developmental efforts to enhance the explosive intelligence (aerial shrewdness) and safety usage of UAV in logistics and other domains. Albeit, this is not without the inherent underlying cognitive intelligence (AI-model) challenges and cybersecurity concerns. With more emphasis on semantic-based schemes [145], neuromorphic strategies [153], minimized information-sharing characteristics [155], and less dependence on GNSS [154] (to improve relative positioning), security situational awareness (SSA) can be achieved. This will accelerate safe UAV navigation for smart logistics.

SSA and prediction are important, especially for UAV battery management and power system measurement. It helps to address routing management, collision avoidance, and inadvertent landing/crashing of UAVs, amongst other security issues associated with UAV usage for logistics (as highlighted in Table 5). Various security factors can be acquired, understood, and predicted thanks to networked-based SSA technology [156]. Figure 9 depicts an SSA scheme for inclusive and decisive UAV positioning, navigation, and timing.

An SSA scheme that will promote smart and safe UAVs for logistics must address aerial vehicles' dynamic scenarios and complexities that match real-world applications while taking into account the hardware-constrained characteristics and the energy efficiency of UAVs' battery systems. Thus, the data sources for scenario testing should undergo quality assurance to reduce bias [12] and ascertain sample variability and feature inclusiveness, such as ego vehicle sensor recordings. Also, adequate feature extraction and engineering are critical for optimal model prediction [12]. Finally, the continuous development of lightweight yet hybrid-based optimization and cognitive algorithms such as scenario description language is essential for proper out-of-the-box semantic analysis of UAV behaviours en route to their destination.

Authors [157] proposed a multi-agent deterministic policy gradient SSA framework for real-time protection of smart grids, which is applicable in addressing attacks in UAV power systems to improve safety navigation. Therefore, developing and applying networked-based SSA technology will aid in the proactive mitigation of security threats aimed at draining UAV batteries through false engagements while en route to their delivery destination. Hence, SSA technology will curtail DoB and DoSp attacks (see Table 7) and improve the smartness and safety navigation of logistics-based UAVs in the airspace, their perception of their immediate environment, and their interaction with surrounding objects. Undoubtedly, advancement in technological capability demands means to ensure continuous trustworthy usage by creating a balance between smartness and safety.

TABLE 9 Performance analysis of cooperative SLAM approaches for UAV safety.

Reference	SLAM type	AI model & algorithm	Safety-based Developmental Strides
Yang et al., (2024) [145]	Semantic visual SLAM	Light-weight DL	Estimates terrain situations through semantic features in real-time (0.407s) for UAV landing guidance.
Friess et al., (2024) [148]	Graph-based SLAM	Iterative close point (ICP)	Entire onboard with 192 kB memory, 0.8 m/s speed, and achieved a mapping accuracy of 12cm for cooperative navigation of 4 nano-UAVs that can be extended to hundreds of UAVs.
Dong et al., (2024) [153]	Bio-inspired visual SLAM	Neuromorphic neural networks	Combines visual-inertial odometry with biological cell models to address the problems of large view disparity, high computational and storage cost, and real-time localization and mapping associated with V-SLAM in heterogeneous UAVs and UGVs, with 0.78m (air) and 2.76m (ground) average localization errors.
Buqing et al., (2024) [149]	Visual SLAM (UAV-UGV cooperation)	Information consensus filter (ICF)	Decentralized control algorithm for real-time safe distance flight control adjustments and inter-UAV communication.
Wang et al., (2024) [150]	Visual SLAM (UAV-UGV cooperation)	Reinforcement learning (RL)	Improved obstacle avoidance and efficient path planning using multi-agent soft actor-critic algorithm for achieving faster task success rate and task completion efficiency
Runmin et al., (2024) [154]	Radio SLAM	Cooperative incremental smoothing and mapping (CI-SAM)	Robust navigation strategies address location divergence issues, self-stabilization, and reduce the need for vehicle measurement to achieve complete relative positioning in the absence of GNSS.
Miguel et al., (2024) [155]	Situational graph-based SLAM using LiDAR	Hierarchical optimization room descriptor and fusion	Decentralized System with minimal trajectory errors and reduced information exchange between UAVs to address the multi-robot kidnapped (hijacking) problem.

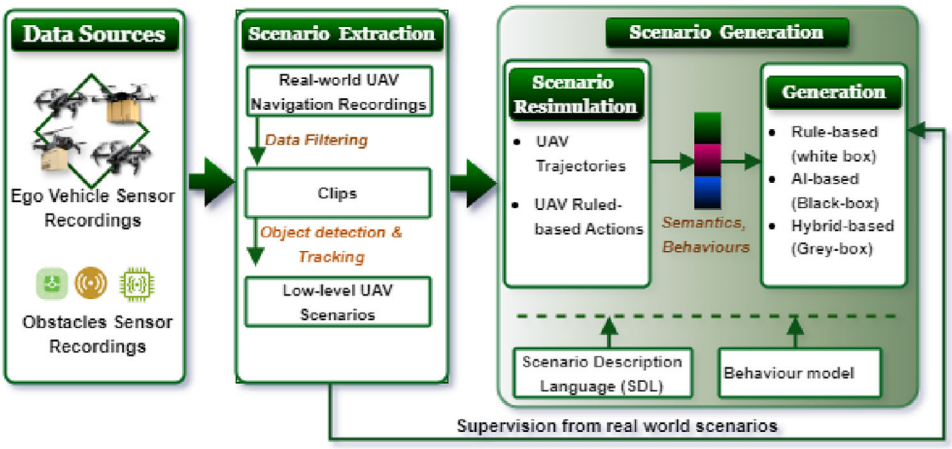

FIGURE 9 Situation-awareness scheme for inclusive and decisive UAV positioning, navigation, and timing.

7 | CHALLENGES AND DIRECTIONS FOR FUTURE UAV SECURITY

The rapid development of uncrewed, connected cars, intelligent transportation, amended vehicles, and other technologies, the on-board electronic system is becoming increasingly complex. This puts higher requirements on the bandwidth and real-time UAV networks [28, 158]. Ultimately, increased complexity leads to increased exposure to risks and vulnerabilities, and demands an unconventional convergence-based approach and connected intelligence to tackle them, and ensure sustainable usage. SMiLE is a complex system burdened with a plethora of security and safety issues (see Table 5), coupled with the inherent challenges of adopting UAVs (see Table 8) to accomplish it. Therefore, the spectral analysis of the security and safety concerns of UAVs for SMiLE indicates that sustainable UAV usage relies on enhanced intelligence capacity to outwit vulnerabilities. Thus, addressing smartness-security intelligence to curtail cyber-attacks, safety-security intelligence for swift navigation, situational-awareness intelligence for scenario-specific landing, and software-centric and storage intelligence for reliable decision-making in package delivery through a transparent cognitive algorithm, tamperproof security approach, and trustworthy architecture is cardinal for the survival or otherwise of UAVs in SMiLE.

The application of explainable AI (XAI) [159], blockchain technology (BTC) [116], and zero-trust architecture

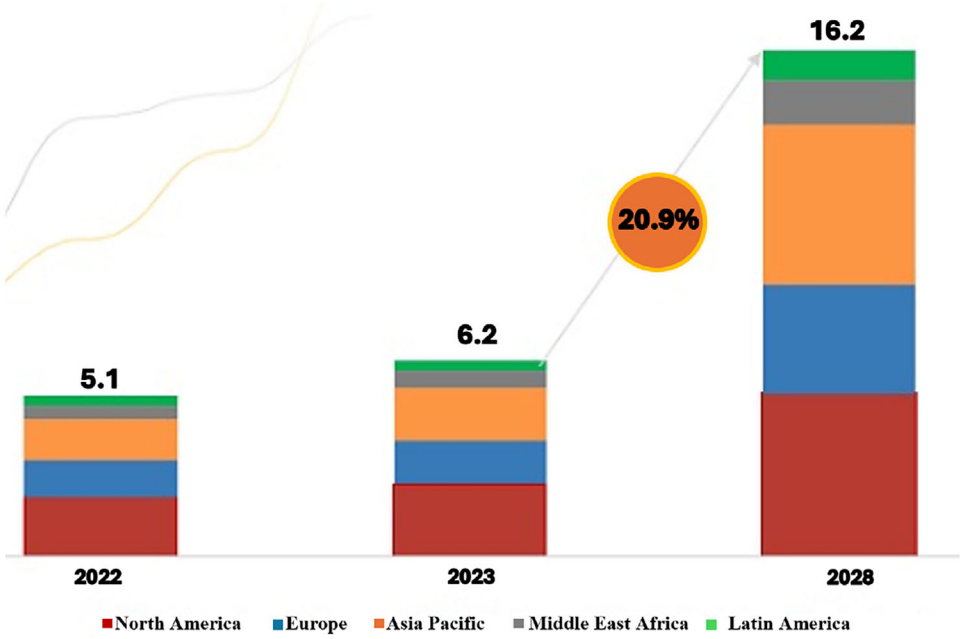

FIGURE 10 XAI growth trajectory and market value.

(ZTA) [160] have proven to be veritable tools for addressing seemingly arduous security issues across domains. This section explores how the convergence of XAI, BTC, and ZTA can be leveraged to address the identified security and safety issues in UAVs for logistics and provide useful research insights for meaningful developments.

7.1 | Transparent interpretation and explainable UAV cognition

Conventional AI models are usually non-transparent and follow "black-box" semantics, which limits practical use-case generalization and makes the interpretability of the models' decisions difficult. As a result, the security and safety concerns associated with UAVs for logistics and aerial mobility can be attributed to inaccurate/false detection of attacks, missed detection of navigation obstacles, misclassification of scenarios and interference, and misinterpretation of results by these underlying AI models [7, 161]. The objective function of the XAI paradigm is to guarantee self-explanatory, reliable, unbiased, and transparent results via ethical AI, valid AI, and interpretable AI [26]. This is to address the intelligence failures associated with UAVs as a result of programmatic conformity and ethnocentric bias [162]. According to [162], XAI shares 0.5% adoption in UAVs when compared with other AI algorithms. Though XAI adoption is relatively nascent (especially in UAVs), the global investment trajectory for technology diffusion and adoption of XAI across different applications was valued at over $20 billion by 2023 [26]. As of 2023, the XAI market size was $6.2 billion, and it is projected to grow by 20.9% resulting in a market value of $16.2 billion by 2028 [163], as seen in Figure 10.

7.1.1 | Advanced intelligence for disruptive UAV mobility curtailment

The industrial application of XAI as the underlying cognitive engine in cyber-physical systems has experienced systematic vertical integration to enhance human-centric processes from industry 1.0 to industry 5.0 revolution [26]. With the local and global explanation approaches of the XAI model, the clarity of the connections between the multifaceted UAV sensors' input-output pairs and the logic of the underlying operations can be understood and validated to decipher intrusions from authorized access into the UAV network. Also, the incorporation of XAI algorithms as the underlying intelligence models in CUAS and SDR will advance the detection, identification, and neutralization of UAVs. It will help to address smartness-security as well as safety security issues such as payload security, drone hijacking, identity theft, package delivery identification, physical hazards etc., as listed in Table 5. [159] integrated ZTA and XAI algorithms for advanced classification of UAVs based on RF signals from three (3) UAV models using shapley additive explanations (SHAP) and local interpretable model-agnostic explanations (LIME) to achieve transparent decision-making and trustworthy interpretation of predictions by the model. Though the outcome was impressive, the use of a single detection technique (RF signal only) rather than a hybrid method (sensor fusion) limits the approach for robust use-case application in ensuring UAV security and safety. Thus, more research efforts directed towards the integration of interpretable AI for hybrid-based multi-class UAV security are solicited will boost trustworthy operations.

Furthermore, to guarantee public safety and UAV intelligence, surveillance, and reconnaissance, it is pertinent that

the hardware and software design of an ML-enabled multi-sensor-SDR (see Figure 5 in Section 4) incorporate XAI as the underlying cognitive model for its different wireless technologies, such as cognitive radios, frequency hopping spread spectrum, and mesh networking. This will enhance the capacity of self-healing networks of UAVs for semantic-driven situation analysis and environment-awareness navigation, as well as improve the scenario-specific neutralization capacity of CUAS systems. Furthermore, it will aid in guarding against the malicious deployment of UAVs to disrupt aerial autonomous vehicular mobility, that endangers the sustainability of UAS applications.

7.1.2 | Accentuated interpretability of interoperable UAV sensor signals

UAV sensor-based attacks (a subset of UAV network cyber-attacks) are attributed to the weaknesses in the underlying conventional AI models for efficient complex signal analysis and processing. Generally, most IDS models (see Table 8) rely on the texture information of UAV signals to detect anomalies aimed at disrupting the UAV movement. However, textual information is insufficient to fully decipher signal anomaly patterns, especially as complexity increases due to multiple sensor fusion coupled with the velocity of dynamic changes in scenarios that often characterize a UAV network. Though DL models can discover patterns from complex scenarios [39], they lack useful information on the underlying process to final prediction, which makes them vague and leaves room for doubt about the authenticity of their results. With the local explanation approach of XAI (LIME), this vagueness of DL predictions of UAV sensor-based attacks can be addressed. The LIME provides a comprehensive and comprehensible interpretation of the underlying operations of a DL model in producing a valid and unbiased prediction [26]. As seen in Figure 8 and Table 8, a software-centric AI-empowered cross-layer security architecture (SACA) for resilient cyber-intelligence in UAV networks must integrate lightweight XAI-based DL models as its intelligence base to drive the software-hardware interactions and decisions of IDS, IPS, and other security technologies enabling UAV mobility. This will certainly reduce GPS spoofing and jamming, thereby preventing UAV hijacking, package delivery diversion, and exploitation of UAVs to disrupt/destroy key infrastructures such as power lines, telecommunication towers etc. More research to develop lightweight XAI-empowered, security technologies is recommended to increase safe and trustworthy UAV autonomy

7.1.3 | Agile requirements for XAI adoption in safety-conscious UAV mobility

The fundamental pillars for transparent and reliable safety-driven cognition for autonomous vehicle networks encompass interpretability, explainability, justifiability, traceability, and transparency in the decision-making process. According to the National Institute of Standards and Technology (NIST) AI risk management [164], a trustworthy AI model must be (i) fair with harmful bias management (ii) privacy-enhanced (iii) explainable and interpretable (iv) accountable and transparent (v) secure and resilient (vi) safe, and (vii) valid and reliable. In using XAI as the underlying cognitive model in UAVs, three requirements are necessary to achieve trustworthy and reliable safety-conscious UAV mobility for logistics. These are data requirements, conventional AI model requirements, and agency requirements. According to [27] data requirements encompass privacy and data governance, diversity, non-discrimination, and fairness. On the other hand, conventional model requirements include technical robustness and safety, security, and resilience, while human agency requirements entail scalable human-machine interfaces for rational decision-making in response to out-of-scale dynamic scenarios. Figure 11 depicts an agile XAI-enabled framework (AXAI) for inclusive safety-conscious UAV mobility for logistics.

The AXAI framework emphasizes explicit interpretation and explanation of all cognition-based UAV activities; perception, planning, and control to ensure reliable and transparent prediction. With these in place, attacks at different layers of the UAV (component, communication, and architecture) can be significantly curtailed. Therefore, the development and integration of AI models into UAV designs that embrace XAI features is a sure bet toward accelerating secure, safety-driven, and sustainable UAV mobility for logistics. Further research directed at addressing these needs is a plus for safety-conscious trustworthy autonomous aerial mobility.

7.2 | Blockchain for tamperproof and traceable UAV control

Protecting the engine room (the intelligence hub) that controls the navigation protocols and principles of UAV decisions is critical for internal and external security. An aerial security design that can guarantee maximum security against malicious UAV mobility as an aerial smart vehicular technology for logistics and other purposes requires an inclusive robustness that blends scalability with speed and security in carrying out real-time (timely), scenario-specific (tactile), traceable (tractable), and trustworthy (transparent) and tamperproof operations that aligns with the SDG. The incorporation of blockchain technology into existing UAV networks is to provide a safe, decentralized, and tamper-proof platform for storing and transmitting sensitive data. Blockchain has the potential to revolutionize data security in UAV user and package authentication [165]. According to [7], the role of BTC in UAV operations cuts across authentication, authorization, and availability of communication in UAV network in carrying out the three main activities of a CUAS design (DIN), with a resultant effect of increase in safety deployment. This tripartite role of transparent BTC in promoting secured and safe UAV mobility is succinctly captured by the regression

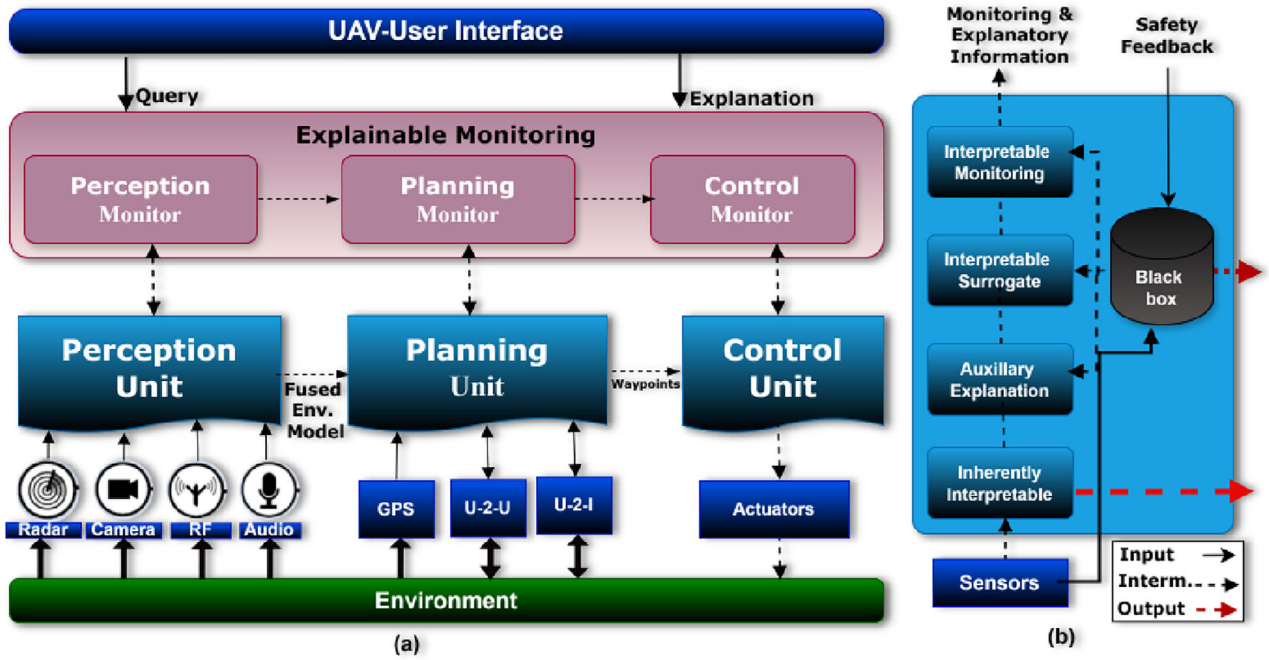

FIGURE 11 Agile XAI framework for safety-driven UAV mobility comprising (a) module for intelligible explanations to achieve trustworthy monitoring and feedback and (b) modular units for specific task interpretations.

model in Equation (1).

$$\alpha \mathrm{Ut_s} = \left[\beta_0 + \beta_1 \mathrm{A_1}^{\mathrm{x}} + \beta_2 \mathrm{A_2}^{\mathrm{y}} + \beta_0 \mathrm{A_3}^{\mathrm{z}} + \cdots + \beta_{\mathrm{n}} \mathrm{A_n}^{\infty} + \in_1\right], \tag{1}$$

where $\alpha \mathrm{Ut_s}$ represents secured UAV; $\mathrm{A_1^x}, \mathrm{A_1^y}, \mathrm{A_1^z} \ldots \mathrm{A_n^\infty}$ stands for authentication, authorization, accountability, and any other emerging security measure for enhanced intelligence space, cyberspace, and airspace; β_0 is the constant security value for applying BTC to UAV operations when values of A are set to 0; β_1, β_2, β_3 $\cdots$ β_{n} are the net regression coefficient security value for applying BTC in UAV operations with dynamic change in A values; and $\in_1$ represents the likely loopholes and emerging issues to be introduced by blockchain. Timeliness has remained the main challenge to integrate BTC into UAV network operations [7].

However, several works have demonstrated that BTC can provide adequate security in UAV networks without sacrificing the performance of the UAV FANET [166–169]. Thanks to the developments of better and faster blockchain decision-making protocols as consensus algorithms Notably, authors [116] proposed the integration of BTC to enhance drone user and package delivery authentication and authorization as seen in Figure 12.

The emergence of newer BTC consensus algorithms (with reduced gas costs) coupled with the introduction of offline transaction capacity has led to its rapid deployment as a frontline security masterpiece in addressing UAV network and mobility security challenges [167]. To be precise, the integration of BTC into IoD-based logistics has resulted in mutual authentication of identity, non-repudiation of delivery and arrival time, and other intangible security benefits [168]. Some key areas of BTC adoption for secured UAV-based logistics and open issues are presented forthwith.

7.2.1 | Seamless UAV user & package delivery authentication

Efficient authentication of UAV users for secure message delivery to prevent physical hijacking of UAVs remains a challenge. Using physical unclonable functions (PUFs) to store UAV device private keys exposes them to privacy leakages. With blockchain, lightweight unified management, decentralized storage of UAV user identity, and simultaneous dynamic updates of private keys can be accomplished. [170] developed a tamper-proof hierarchical blockchain-based dynamic secret key strategy for the swarms of UAVs that eliminates the need to store any secret information within UAVs, thereby mitigating the vulnerabilities associated with key leakages resulting in physical attacks. This ensures complete decentralization of the authentication process, data transparency, and a tamper-proof security protocol with reduced computation and communication overhead suitable for resource-limited UAV systems. [171] proposed BETA-UAV; a blockchain-trust authentication scheme for resisting active attacks such as replaying, impersonation, and modification with lightweight computational and communication overhead costs. Furthermore, BTC can be integrated to track package deliveries from the inception point to the target delivery destination. Authors [116] developed a robust CUAS that uses BTC to verify and authenticate the legitimacy of a drone operation and verify its package delivery to forestall possible disruption via malicious attacks. The system

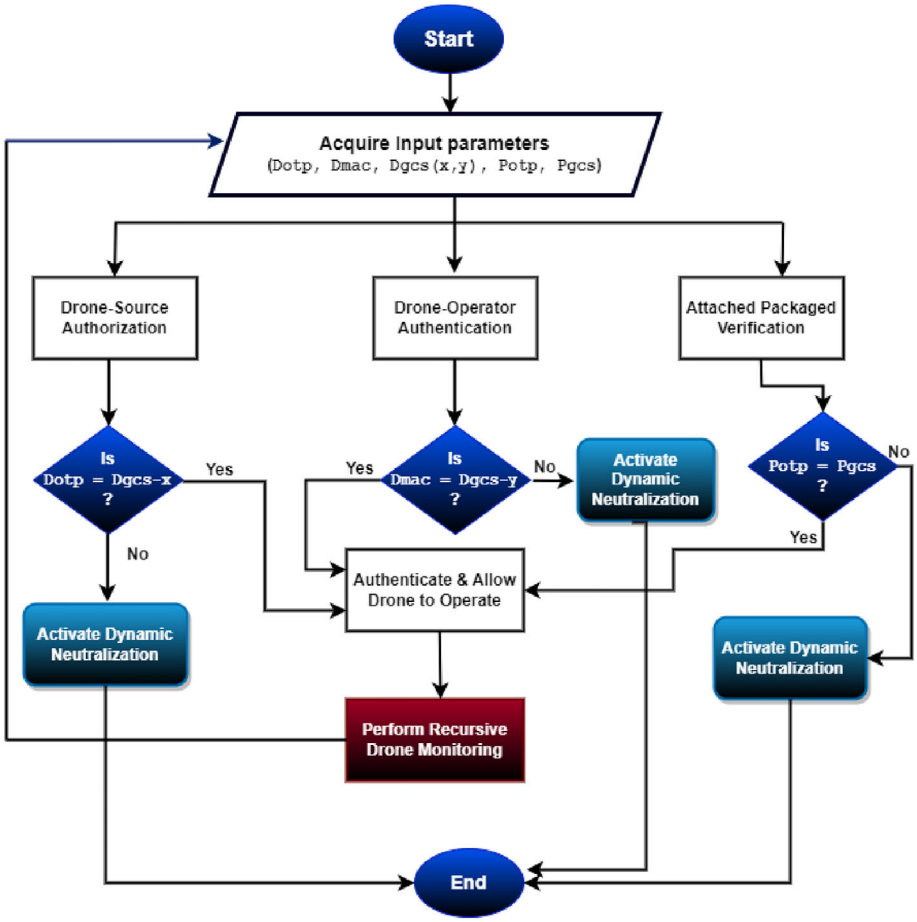

FIGURE 12 Flowchart of blockchain-empowered CUAS for UAV-based logistics authentication and validation for (a) drone source authentication, (b) drone operator authentication, and (c) attached package verification [116].

accepts inputs about the drone information and attached package in real-time over the cloud, verifies them using a proof of authority algorithm and smart contract, and authenticates them using a decentralized application that is deployed on the drone, the GCS, and the CUAS, before executing the appropriate neutralization response.

7.2.2 | Surrogate UAV navigation authorization

Blockchain guarantees data integrity through decentralized ledger security (storage security) and access control for collaborative UAV swarm navigation through data sharing [167]. With BTC, UAV system adaptability to the network fluctuation consequent upon potential cyber-attacks by masqueraders can be mitigated by evaluating the signal parameters and characteristics, adjusting the trust propagation, and updating strategies accordingly. Authors [172] proposed a data-trustworthy interconnection platform that combines AI algorithms, smart contracts, and BTC consensus algorithms to achieve a real-time secure situational awareness system for a cluster of interconnected UAVs operating in an environment. This result demonstrates the feasibility of efficient and effective secured data sharing and transmission in UAV networks for improved logistics and cyber-attack curtailment, especially routing protocol attacks such as ID spoofing, hijacking, DoS/DDoS, SQL injection, and NoSQL injections. Also, to address attacks associated with UAV node failures (such as tampering, DoS, spoofing etc.), authors [173] proposed a combination of delegated proof of stake (DPoS) and practical byzantine fault tolerance (PBFT) consensus algorithm to achieve a balance between efficiency, resilience, and security against UAV node failures. Further research focused on incorporating geospatial smart contracts, privacy-preserving data sharing, and deep reinforcement learning, into the existing BTC proposals will complement the progress recorded toward secured and safe UAV navigation.

7.2.3 | Streamlined UAV communication availability via secured data exchange

UAVs only move within the control range of the GCS due to inadequate network coverage and latency. Also, U-2-U communications are restricted by distance and often exposed to multiple attacks. With the convergence of BTC and 6G technologies, ubiquitous control of UAV communication availability can be streamlined with expanded network capacity and security for efficient task performance. Authors [174] proposed

a ubiquitous UAV task security management architecture that combines BTC and 6G for FANETs using a distributed control network (DCN), rapid consensus mechanism (RCS), and a UAV emergency consensus mechanism to ensure data consistency and authenticity of entities. This result indicates that while the RCS achieves quick data consistency, for DCN, the UAV-emergency provides secure data support for the cross-regional control of UAV formations in the FANET. However, AI algorithms need to be introduced to achieve faster processing of distributed data for parallel execution of UAV tasks to match the security characteristics for improved performance. Besides, 6G technology can also be applied in DCN and combined with AI algorithms to achieve highly reliable, low-latency transmission and safe and fast processing of distributed data to accelerate the execution of UAV tasks. Furthermore, BTC can be leveraged to address adversary attacks on centralized cloud computing-based storage data availability and scalability. [127] proposed a lightweight hyper ledger blockchain-based authentication scheme (LAKA-UAV) to ensure access control and data integrity. The result demonstrates that as the number of transactions increases (due to an increase in the number of mining blocks), efficient computational time is maintained when compared with legacy security architecture. Therefore, more research and development towards the combination of lightweight BTC and AI-empowered UAV network solutions will accelerate secured and sustainable UAV usage for logistics.

7.2.4 | Requirement for scalable blockchain application in UAV-based logistics

The adoption of blockchain technology into a time-sensitive mission-critical cyber-physical system such as UAV network is often confronted with maintaining a balance between security, speed, and scalability (SSS) requirements [7], that is in tandem with the energy-efficiency consciousness and hardware resource constraints characteristics of UAVs. These SSS requirements cut across technical (hardware and software requirements), regulatory (governance requirements), and operational (end-user requirements) domains to guarantee seamless and streamlined confidentiality, integrity, and availability. Integrating BTC into a UAV-based logistics ecosystem introduces several requirements for effective adoption.

1. **Immutable data integrity**: The BTC ledger must ensure that shipments, routes, and inventory data cannot be altered to maintain trustworthy transactions and event records.
2. **Interoperability with legacy systems**: BTC solutions for UAV-based logistics must be compatible with existing logistics management software and supply chain networks for seamless data exchange and integration.
3. **Intelligent automation of smart contract**: Smart contracts embedded with predefined rules and conditions that control all operations and trigger event-based and time-based actions must be robust and rational to accommodate all security aspects of the logistics operations and navigation.
4. **Identifiable supply chain**: Visible tracking of the current status of the UAV movement and attached package must be incorporated into the blockchain-enabled solution for UAV-based logistics.
5. **Inclusive data privacy protection**: BTC-enabled solutions should have decentralized mechanisms for robust privacy-preservation of sensitive logistics information from unauthorized access.
6. **Informative monitoring and interventions**: Informed real-time feedback and updates are essential for timely and proactive interventions in logistics processes to improve the quality of service. The BTC solution should provide a visible means for proactive decision-making, especially in re-directing the UAV mobility towards priority zones.
7. **Innocuous scalability**: As an extension of the SMiLE, the adoption of BTC in UAV-based logistics should extend the capacity of the system to handle big data from transactions emanating from multiple sources without jeopardizing the integrity of the system nor restrict its compatibility with other logistics processes.
8. **Intrinsic regulatory compliance**: The BTC security design must adhere to established regulatory frameworks and standards to avoid conflicts with the existing governance policies on airspace operations
9. **Incremental cost effectiveness**: Considering the cost implication of adopting new technology, the BTC design should strive to guarantee overhead costs, improved operational efficiency, high return on investment, and overall customer satisfaction in the long term.

Meeting these requirements demands close collaboration between the stakeholders and key decision-makers in the SMiLE such as IT and security professionals, drone manufacturers, logistics companies, regulators, and the end-users of the system.

7.3 | Zero-trustworthy and tractable UAV cooperation

Zero trust (ZT) is an evolving set of cybersecurity paradigms that move defences from static, network-based perimeters to focus on users, assets, and resources [175]. ZT architecture (ZTA) adopts ZT principles and policies to plan enterprise infrastructure and industrial workflows with the assumption that no implicit trust is granted to assets or user accounts based solely on their physical or network location (the Internet of local area network) or based on asset ownership (personal or enterprise-based). Hence, authentication and authorization are performed discretely, and an enterprise resource is established. According to the NIST special report [175], ZTA focuses on protecting resources (assets, workflows, services, network accounts etc.) and not the network segments since the network location is no longer considered an integral component to the security standpoint of the resource. ZTA is a response to enterprise network trends such as remote users, the connect your device (interoperability) concept, and cloud-based assets

that are located outside the boundary of the enterprise network. This is analogous to UAV FANET characteristics (refer to Section 5). ZTA is not a single architecture but a consortium of guiding principles for system design, workflow, and operations that can be used to improve the sensitivity level or classification of any security posture. Therefore, ZTA can be adopted as a revolutionary way to address the growing security risks posed by UAV usage for logistics, as it can substantially reconceptualize conventional security models by promoting a constant and thorough verification of all entities inside a network environment, thereby eliminating implicit trust.

The core tenet of ZTA is "never trust, always verify," meaning that even within trusted zones of operation, resource access must be explicitly granted [176]. This transition is vital within the realm of UAV operations, where the ever-changing and frequently unforeseeable characteristics of flight paths and interactions require a security framework that is more robust and flexible. Although there is a clear need for it, the integration of ZTA in UAV security is still in its early stages because it is a journey that is implemented incrementally based on risk factors, process changes, and the use-case of technological solutions. One particular problem of transitioning into ZTA for UAV operation is establishing continuous authentication mechanisms that can keep up with the changing operational dynamics of UAVs. Traditional security tactics frequently prove insufficient. This is either due to their lack of flexibility or their failure to effectively handle the full range of possible dangers posed by UAVs. A few use cases of the adoption of ZTA in UAV security reveal the potential of the zero-trust cybersecurity paradigm for UAV resource protection to ensure data security, user identity, access management, operations, endpoint validation, and host environment authentication.

In ref. [177] adopted ZTA to develop a rapid UAV user-identity authentication scheme for trustworthy and highly tractable UAV swarm cooperation, to address vulnerabilities such as identity counterfeiting, illegal eavesdropping, tampering, reply attacks, man-in-the-middle, or DiTM, and forgery attacks. Their scheme ensured speedy data exchange and sharing links, thereby strengthening the ability of UAV nodes to connect intelligibly in a transparent manner. To tackle leakage attacks (such as injections and spoofing) associated with exposure of people's identities during package delivery, [178] adopted ZTA for continuous authentication of UAV delivery. The scheme entails continuous authentication, multi-factor authentication, and digital authentication using self-sovereign identity techniques—a blockchain-based approach. Authors [159] combined XAI and ZTA to enhance UAV security through a rigorous and continuous process of authenticating all the network entities and communications. With this approach, all the participating UAVS within the network are comprehensively verified to enhance security in the UAV network. Furthermore, to improve the prediction reliability of IDS, authors [179] proposed a ZTA-empowered IDS that combines security rules and ML algorithms for cooperative detection and curtailment of cyber-attacks on IoD. However, these attempts lacked practical implementations, as most were either simulation-based or concept-based.

7.3.1 | Key consideration & requirements for ZTA adoption in UAV-based logistics

From the foregoing, it is evident that ZTA as a cybersecurity paradigm in safety-driven UAV-based logistics focuses on authentication and authorization, and shrinking implicit trust zones while maintaining availability and minimizing temporal delays in the authentication strategies. Succinctly put; prevent unauthorized access to data and services, and make access control enforcement as granular as possible. This prevention and enforcement has to be carried out in the three core components of a logical ZTA as seen in Figure 13 namely policy engine (PE), policy administrator (PA), in the control plane, and policy enforcement point (PEP) in the data plane.

The PE takes the ultimate decision of granting access to a resource for a given user. The PA establishes and/or revokes communication between the resource and the user, while the PEP enables, monitors, and eventually terminates the connection between the user and the resource. To implement ZTA for improved safety-driven and security-conscious UAV-based logistics, seven (7) fundamental considerations must be adhered to in line with the ZTA core tenets.

1. All data sources and computing services are considered resources. A UAV network may comprise multiple UAVs with different models and sizes. Each UAV network may have means to send to and exchange data from an aggregate storage source. The enterprises may have the means to classify the UAVs/categories.
2. All communication is secured, regardless of network location. Access requests from enterprise networked infrastructure (i.e. UAV to Infrastructure) must have the same security requirements as access requests and communication from the non-enterprise-based network (UAV-to-UAV).
3. Access to individual enterprise resources is granted on a per-session basis. The UAV user's request must be evaluated before access is granted. That is, access is granted to the least privileges needed to complete a task.
4. Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioural and environmental attributes. Data governance rules must be in place to define what resources are available, who can access them, and what level of access each user can get.
5. The enterprise monitors and measures the integrity and security posture of all owned and associated assets. No participating node in the UAV network is inherently trusted. The security system strategy must evaluate the security posture of each participating UAV when evaluating a resource request. In other words, the system must establish continuous diagnostics and monitoring of the current status of all devices and applications in the network to provide actionable data about the current state of the UAV network.
6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed. To implement ZTA in UAV network, the system must have an

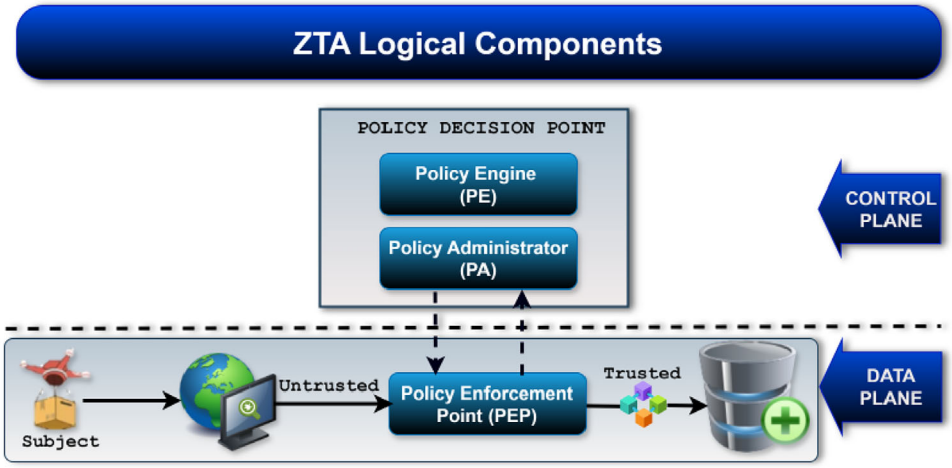

FIGURE 13 Zero trust architecture highlighting the three core logical components: (a) policy engine (PE), (b) policy administrator (PA), in the control plane, and (c) policy enforcement point (PEP) in the data plane.

identity, credential, and access management (ICAM) and asset management framework in place. That is, there must be a multi-factor authentication, re-authentication, and re-authorization mechanism for continuous monitoring and feedback.

7. The enterprise collects as much information as possible about the current state of assets, network infrastructure, and communications and uses it to improve its security posture The system should have means to collect data about the security posture of the system, network traffic, and access requests, then process the data to discover insights, and use the gained insights to provide context-based and situation-awareness requests from participating nodes in the UAV network.

Implementing the ZTA cybersecurity paradigm to accelerate safety-driven UAV, enhanced identity governance, micro-segmentation, and/or network infrastructure-software defined parameter-based approaches can be adopted depending on the security needs and in line with these fundamental requirements. These fundamental considerations connote that the various systemic vulnerabilities, security attacks, and safety issues associated with the use of UAV for logistics can be sufficiently addressed using ZTA to maintain security governance, BTC for tamper-proof decentralized data storage, and XAI for reliable and transparent interpretation of the discovered insights for context-aware decision making in UAV networks. However, these ZTA tenet requirements are technology agnostic; meaning several underlying factors and relationships between participating entities need to be established. This is to guarantee robust integration and implementation to enhance the security posture of any enterprise-driven network, such as a UAV network for logistics. Research efforts targeted at establishing a robust framework for the widespread adoption and scalable integration of ZTA, BTC, and XAI in autonomous vehicles (especially UAVs) are necessary to improve the security and safety-driven performance of UAVs as priority-based logistic vehicles. Thereby enhancing the capacity of a smart and intelligent logistics ecosystem. Therefore, the proposed UAV for smart mobility and intelligent logistics ecosystems (U-SMiLE) framework needs to have a robust cross-layer-multi-factor security feature that is supported by blockchain immutability, driven by an XAI-empowered application for context-aware and trustworthy decision-making. Importantly, this has to be controlled by the security governance established on the core principles of zero-trust architecture.

8 | CONCLUSION

The use of UAVs for smart mobility and intelligent logistics is gaining widespread adoption due to technological diffusion and advancements in underlying UAV technologies such as increased payload capacities, longer flight times, situational awareness cognition etc. However, this scalable adoption is confronted with myriads of security and safety issues threatening the usability, viability, and continual existence of UAVs in enhancing the capacity of SMiLE. This review examined the spectrum of existing and emerging security and safety issues associated with UAV usage for logistics. Also, it delved into the strategies for effective security and efficient safety-driven smartness in UAV networks and operations. Furthermore, it explored the vital role of explainable AI algorithms for transparent context-aware cognition intelligence, the place of blockchain technology for tamperproof security control intelligence, and the importance of zero-trust architecture for trustworthy core governance cooperation intelligence. The convergence of these technologies is pivotal in addressing the risks associated with UAV usage and facilitating safety-conscious and scalable UAV deployment for smart logistics. Thereafter, it delved into key requirements and considerations for integrating these intelligence paradigms in UAV operations.

It is evident from the review outcome that security issues in UAV-based logistics cut across airspace security, cybersecurity,

data privacy, payload security, and infoswarm-a multifaceted cyber-cognitive issue. On the other hand, safety issues include inadvertent landing, airspace accidents, and collisions, disruptive tendencies of key infrastructures etc. At the surface level, attacks on UAVs are targeted at their communication layer (network, transport, and physical layers), communication architecture (UAV-to-UAV, UAV-to-infrastructure), and physical components (hardware, software, and sensors), with routing protocol attacks being the dominant attacks on UAV-based logistics. Integrating conventional security and AI algorithms in UAVs presents room for improvement. Addressing this plethora of issues requires a convergence approach to tackling multi-dimensional scenarios. By adopting the potential of zero trust architecture to maintain security governance, blockchain for tamper-proof decentralization data storage, and explainable AI algorithms for reliable and transparent interpretation of the discovered insights for context-aware decision-making in UAV networks and logistics operations. However, the integration of zero trust, blockchain, and explainable AI to enhance the security and safety of UAV mobility and networks is technology agnostic. Therefore, different use-case requirements should be considered for the scalable adoption of these tripod paradigms to accelerate the capacity of smart mobility and intelligent logistic ecosystems via UAV.

AUTHOR CONTRIBUTIONS

Simeon Okechukwu Ajakwe and Dong-Seong Kim: Review and editing (equal); conceptualization (equal); writing—review and editing (equal). **Simeon Okechukwu Ajakwe**: Writing—original draft (lead); formal analysis (lead); writing—review and editing (equal); methodology (lead); conceptualization (supporting); writing—original draft (supporting).

ACKNOWLEDGEMENTS

This research was partly supported by Innovative Human Resource Development for Local Intellectualization program through the Institute of IITP grant funded by the Korean government (MSIT) (IITP-2024-RS-2020-II201612, 33%) and by Priority Research Centers Program through the NRF funded by the MEST (2018R1A6A1A03024003, 33%) and by the IITP (Institute of Information & Communications Technology Planning & Evaluation)-ICAN (ICT Challenge and Advanced Network of HRD) grant funded by the Korea government (Ministry of Science and ICT) (IITP-2024-2022-00156394*, 34%).

CONFLICT OF INTEREST STATEMENT

The authors declare no conflicts of interest.

DATA AVAILABILITY STATEMENT

Data sharing is not applicable—no new data is generated, or the article describes entirely theoretical research.

ORCID

Simeon Okechukwu Ajakwe https://orcid.org/0000-0002-6973-530X
Dong-Seong Kim https://orcid.org/0000-0002-2977-5964

REFERENCES

1. Savithramma, R., Ashwini, B., Sumathi, R.: Smart mobility implementation in smart cities: a comprehensive review on state-of-art technologies. In: 2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT), pp. 10–17. IEEE, Piscataway, NJ (2022)
2. Singh, S.: Smart Cities – A$1.5 Trillion Market Opportunity. Forbes/Business https://www.forbes.com/sites/sarwantsingh/2014/06/19/smart-cities-a-1-5-trillion-market-opportunity/. Accessed 30 Mar 2024
3. Li, J., Qin, R., Olaverri-Monreal, C., Prodan, R., Wang, F.-Y.: Logistics 5.0: from intelligent networks to sustainable ecosystems. IEEE Trans. Intell. Veh. 8(7), 3771–3774 (2023)
4. Javed, A.R., Shahzad, F., ur Rehman, S., Zikria, Y.B., Razzak, I., Jalil, Z., Xu, G.: Future smart cities: requirements, emerging technologies, applications, challenges, and future aspects. Cities 129, 103794 (2022)
5. Gupta, R., Kumari, A., Tanwar, S.: Fusion of blockchain and artificial intelligence for secure drone networking underlying 5G communications. Trans. Emerging Telecommun. Technol. 32(1), e4176 (2021)
6. Benarbia, T., Kyamakya, K.: A literature review of drone-based package delivery logistics systems and their implementation feasibility. Sustainability 14(1), 360 (2021)
7. Ajakwe, S.O., Kim, D.-S., Lee, J.-M.: Drone transportation system: systematic review of security dynamics for smart mobility. IEEE Internet Things J. 10(16), 14 462–14 482 (2023)
8. Josef, F., Jon, G.: Israel says iran launched more than 300 drones and missiles, 99% of which were intercepted. https://apnews.com/article/strait-of-hormuz-vessel-33fcffde2d867380e98c89403776a8ac (2024). Accessed 5 Mar 2024
9. Wu, J., Guo, S., Huang, H., Liu, W., Xiang, Y.: Information and communications technologies for sustainable development goals: state-of-the-art, needs and perspectives. IEEE Commun. Surv. Tut. 20(3), 2389–2406 (2018)
10. Mao, S., He, S., Wu, J.: Joint UAV position optimization and resource scheduling in space-air-ground integrated networks with mixed cloud-edge computing. IEEE Syst. J. 15(3), 3992–4002 (2020)
11. Wen, H., Tang, J., Wu, J., Song, H., Wu, T., Wu, B., Ho, P.-H., Lv, S.-C., Sun, L.-M.: A cross-layer secure communication model based on discrete fractional fourier fransform (DFRFT). IEEE Trans. Emerging Top. Comput. 3(1), 119–126 (2014)
12. Ajakwe, S.O., Opeyemi, D.-O., Samuel, O., Francis, D., Israel, B.: Multidimensional perspective to data preprocessing for model cognition verity: Data preparation and cleansing - approaches for model optimal feedback validation. In: Kumarir, A. (ed.) Recent Trends and Future Direction for Data Analytics, pp. 15–57. IGI Global, Hershey, PA (2024)
13. Young, L.: A multi-modality mobility concept for a small package delivery UAV. AHS International Technical Meeting on VTOL Unmanned Systems and Autonomy no. ARC-E-DAA-TN38630 (2017). https://ntrs.nasa.gov/citations/20180002627. Accessed 5 Apr 2024
14. Sharma, A., Vanjani, P., Paliwal, N., Basnayaka, C.M., Jayakody, D.N.K., Wang, H.-C., Muthuchidambaranathan, P.: Communication and networking technologies for UAVs: a survey. J. Network Comput. Appl. 168, 102739 (2020)
15. Alwateer, M., Loke, S.W.: Emerging drone services: challenges and societal issues. IEEE Technol. Soc. Mag. 39(3), 47–51 (2020)
16. Kumari, A., Gupta, R., Tanwar, S., Kumar, N.: A taxonomy of blockchain-enabled softwarization for secure UAV network. Comput. Commun. 161, 304–323 (2020)
17. Mehta, P., Gupta, R., Tanwar, S.: Blockchain envisioned UAV networks: challenges, solutions, and comparisons. Comput. Commun. 151, 518–538 (2020)
18. Yaacoub, J.-P., Noura, H., Salman, O., Chehab, A.: Security analysis of drones systems: attacks, limitations, and recommendations. Internet Things 11, 100218 (2020)
19. Issaoui, Y., Khiat, A., Bahnasse, A., Ouajji, H.: Toward smart logistics: engineering insights and emerging trends. Arch. Comput. Methods Eng. 28, 3183–3210 (2021)
20. Labib, N.S., Brust, M.R., Danoy, G., Bouvry, P.: The rise of drones in internet of things: a survey on the evolution, prospects and

challenges of unmanned aerial vehicles. IEEE Access 9, 115 466–115 487 (2021)
21. Li, Y., Liu, M., Jiang, D.: Application of unmanned aerial vehicles in logistics: a literature review. Sustainability 14(21), 14473 (2022)
22. Chiper, F.-L., Martian, A., Vladeanu, C., Marghescu, I., Craciunescu, R., Fratu, O.: Drone detection and defense systems: survey and a software-defined radio-based solution. Sensors 22(4), 1453 (2022)
23. Gohari, A., Ahmad, A.B., Rahim, R.B.A., Supa'at, A., Abd Razak, S., Gismalla, M.S.M.: Involvement of surveillance drones in smart cities: a systematic review. IEEE Access 10, 56611–56628 (2022)
24. Wang, L., Deng, X., Gui, J., Jiang, P., Zeng, F., Wan, S.: A review of urban air mobility-enabled intelligent transportation systems: mechanisms, applications and challenges. J. Syst. Archit. 141, 102902 (2023)
25. Ceviz, O., Sadioglu, P., Sen, S.: A survey of security in UAVs and FANETs: issues, threats, analysis of attacks, and solutions. arXiv:2306.14281 (2023)
26. Trivedi, C., Bhattacharya, P., Prasad, V.K., Patel, V., Singh, A., Tanwar, S., Sharma, R., Aluvala, S., Pau, G., Sharma, G.: Explainable AI for Industry 5.0: vision, architecture, and potential directions. IEEE Open J. Ind. Appl. 5, 177–208 (2024)
27. Kuznietsov, A., Gyevnar, B., Wang, C., Peters, S., Albrecht, S.V.: Explainable AI for safe and trustworthy autonomous driving: a systematic review. arXiv:2402.10086 (2024)
28. Quadar, N., Chehri, A., Debaque, B., Ahmed, I., Jeon, G.: Intrusion detection systems in automotive ethernet networks: challenges, opportunities and future research trends. IEEE Internet Things Mag. 7(2), 62–68 (2024)
29. Alquwayzani, A.A., Albuali, A.A.: A systematic literature review of zero trust architecture for UAV security systems in IoBT (2024). https://doi.org/10.20944/preprints202403.0349.v1
30. Sakthivel, V., Patel, S., Lee, J.W., Prakash, P.: Drone delivery. Drone Technology: Future Trends and Practical Applications, pp. 425–440. Wiley, New York, NY (2023)
31. Federal Aviation Administration: UAS sightings report. https://www.faa.gov/uas/resources/public_records/uas_sightings_report (2024)
32. Fraga-Lamas, P., Ramos, L., Mondéjar-Guerra, V., Fernández-Caramés, T.M.: A review on IoT deep learning UAV systems for autonomous obstacle detection and collision avoidance. Remote Sens. 11(18), 2144 (2019)
33. Castrillo, V.U., Manco, A., Pascarella, D., Gigante, G.: A review of counter-UAS technologies for cooperative defensive teams of drones. Drones 6(3), 65 (2022)
34. Krishna, C.L., Murphy, R.R.: A review on cybersecurity vulnerabilities for unmanned aerial vehicles. In: 2017 IEEE International Symposium on Safety, Security and Rescue Robotics (SSRR), pp. 194–199. IEEE, Piscataway, NJ (2017)
35. Patterson, M.D., Quinlan, J., Fredericks, W.J., Tse, E., Bakhle, I.: A modular unmanned aerial system for missions requiring distributed aerial presence or payload delivery. In: 55th AIAA Aerospace Sciences Meeting, pp. 1–14. AIAA Publications, Washington, D.C. (2017)
36. Kallenborn, Z.: InfoSwarms: drone swarms and information warfare. Parameters 52(2), 87–102 (2022)
37. Ajakwe, S.O., Ihekoronye, V.U., Kim, D.-S., Lee, J.-M.: ALIEN: assisted learning invasive encroachment neutralization for secured drone transportation system. Sensors 23(3), 1233 (2023)
38. Boukoberine, M.N., Zhou, Z., Benbouzid, M.: A critical review on unmanned aerial vehicles power supply and energy management: solutions, strategies, and prospects. Appl. Energy 255, 113823 (2019)
39. Ajakwe, S.O., Ihekoronye, V.U., Kim, D.-S., Lee, J.M.: DRONET: multi-tasking framework for real-time industrial facility aerial surveillance and safety. Drones 6(2), 46 (2022)
40. Haviv, H., Elbit, E.: Drone threat and CUAS technology: White Pap. Elbit Syst. 1, 1–19 (2019)
41. Ajakwe, S.O., Ihekoronye, V.U., Akter, R., Kim, D.-S., Lee, J.M.: Adaptive drone identification and neutralization scheme for real-time military tactical operations. In: 2022 International Conference on Information Networking (ICOIN), pp. 380–384. IEEE, Piscataway, NJ (2022)
42. Ajakwe, S., Kim, D.S., Lee, J.-M.: Radicalization of airspace security: prospects and botheration of drone defense system technology. J. Intell., Conflict, Warf. 6(1), 23–48 (2023)
43. Ajakwe, S., Akter, R., Kim, D., Lee, J.: Lightweight CNN model for detection of unauthorized UAV in military reconnaissance operations. In: Korean Institutes of Communications and Information Sciences Conference, vol. 1, pp. 1–3. Korea Institute Of Communication Sciences, Daejeon (2021)
44. Dini, M.A., Ajakwe, S.O., Kim, D.-S., Lee, J.M., Jun, T.: Droneilliance and detection dynamics: a review of radar techniques and trends. Paper presented at the 2022 Korean institute of communications society (KICS) fall conference, Korea Institute of Communication Sciences, Daejeon, Nov 2022
45. Sazdić-Jotić, B., Pokrajac, I., Bajčetić, J., Bondžulić, B., Obradović, D.: Single and multiple drones detection and identification using RF based deep learning algorithm. Expert Syst. Appl. 187, 115928 (2022)
46. Yavariabdi, A., Kusetogullari, H., Celik, T., Cicek, H.: Fastuav-net: A multi-UAV detection algorithm for embedded platforms. Electronics 10(6), 724 (2021)
47. Roberts, J.M.: The most promising defense against militarized drone swarms. https://mindmatters.ai/2021/06/the-mostpromising-defense-against-militarized-drone-swarms/ (2024). Accessed 8 Apr 2024
48. Ajakwe, S.O., Ihekoronye, V.U., Kim, D.-S., Lee, J.-M.: Tractable minacious drones aerial eecognition and safe-channel neutralization scheme for mission critical operations. In: 2022 IEEE 27th International Conference on Emerging Technologies and Factory Automation (ETFA), pp. 1–8. IEEE, Piscataway, NJ (2022)
49. Ferreira, R., Gaspar, J., Sebastião, P., Souto, N.: A software defined radio based anti-UAV mobile system with jamming and spoofing capabilities. Sensors 22(4), 1487 (2022)
50. Guvenc, I., Koohifar, F., Singh, S., Sichitiu, M.L., Matolak, D.: Detection, tracking, and interdiction for amateur drones. IEEE Commun. Mag. 56(4), 75–81 (2018)
51. Deng, M., Peng, S., Xie, X., Jiang, Z., Hu, J., Qi, Z.: A diffused mini-sniffing sensor for monitoring SO2 emissions compliance of navigating ships. Sensors 22(14), 5198 (2022)
52. Ihekoronye, V.U., Ajakwe, S.O., Kim, D.-S., Lee, J.M.: Mobility-compliant model in drone-based sniffing technique for aerial surveillance and security. https://journal-home.s3.ap-northeast-2.amazonaws.com/site/2022f/abs/QPKHH-0390.pdf (2022)
53. Skorobogatov, G., Barrado, C., Salamí, E.: Multiple UAV systems: a survey. Unmanned Syst. 8(02), 149–169 (2020)
54. Sazdic-Jotic, B., Pokrajac, I., Bajcetic, J., Bondzulic, B., Obradovic, D.: Single and multiple drones detection and identification using RF-based deep learning algorithm. Expert Syst. Appl. 187, 115928 (2022)
55. Romesburg, H., Wang, J., Jiang, Y., Wang, H., Song, H.: Software defined radio based security analysis for unmanned aircraft systems. In: 2021 IEEE International Performance, Computing, and Communications Conference (IPCCC), pp. 1–5. IEEE, Piscataway, NJ (2021)
56. Kafetzis, D., Vassilaras, S., Vardoulias, G., Koutsopoulos, I.: Software-defined networking meets software-defined radio in mobile ad hoc networks: state of the art and future directions. IEEE Access 10, 9989–10 014 (2022)
57. Michailidis, E.T., Maliatsos, K., Vouyioukas, D.: Software-defined radio deployments in UAV-driven applications: a comprehensive review. (2024). https://doi.org/10.1109/OJVT.2024.3477937
58. Basak, S., Rajendran, S., Pollin, S., Scheers, B.: Combined RF-based drone detection and classification. IEEE Trans. Cognit. Commun. Networking 8(1), 111–120 (2021)
59. Gelman, I., Loftus, J., Hassan, A.: Adversary UAV Localization with Software Defined Radio. Worcester Polytechnic Institute, Worcester, MA (2019)
60. Fang, L., Wang, X.H., Zhou, H.L., Zhang, K.: Design of portable jammer for UAV based on SDR. In: 2018 International Conference on Microwave and Millimeter Wave Technology (ICMMT), pp. 1–3. IEEE, Piscataway, NJ (2018)
61. Pärlin, K., Alam, M.M., Moullec, Y.L.: Jamming of UAV remote control systems using software defined radio. In: 2018 International Conference on Military Communications and Information Systems (ICMCIS), pp. 1–6. IEEE, Piscataway, NJ (2018)

62. Nie, W., Han, Z.-C., Li, Y., He, W., Xie, L.-B., Yang, X.-L., Zhou, M.: UAV detection and localization based on multi-dimensional signal features. IEEE Sens. J. 22(6), 5150–5162 (2021)
63. Xu, C., Chen, B., Liu, Y., He, F., Song, H.: RF fingerprint measurement for detecting multiple amateur drones based on STFT and feature reduction. In: 2020 Integrated Communications Navigation and Surveillance Conference (ICNS), pp. 4G1-1–4G-1-7. IEEE, Piscataway, NJ (2020)
64. Nemer, I., Sheltami, T., Ahmad, I., Yasar, A.U.-H., Abdeen, M.A.: RF-based UAV detection and identification using hierarchical learning approach. Sensors 21(6), 1947 (2021)
65. Basak, S., Rajendran, S., Pollin, S., Scheers, B.: Drone classification from RF fingerprints using deep residual nets. In: 2021 International Conference on Communication Systems & Networks (COMSNETS), pp. 548–555. IEEE, Piscataway, NJ (2021)
66. Price, J., Li, Y., Shamaileh, K.A., Niyaz, Q., Kaabouch, N., Devabhaktuni, V.: Real-time classification of jamming attacks against UAVs via on-board software-defined radio and machine learning-based receiver module. In: 2022 IEEE International Conference on Electro Information Technology (eIT), pp. 1–5. IEEE, Piscataway, NJ (2022)
67. Özkaner, A., Akça, Y.: Mini/micro UAV detection in the presence of ISM or spurious signals and an experimental application on an SDR. Eng. Sci. Technol., Int. J. 49, 101591 (2024)
68. Xue, C., Li, T., Li, Y.: Radio frequency based distributed system for non-cooperative UAV classification and positioning. J. Inf. Intell. 2(1), 42–51 (2024)
69. Scazzoli, D., Moro, S., Teeda, V., Upadhyay, P.K., Magarini, M.: Experimental comparison of UAV-based RSSI and AOA localization. IEEE Sens. Lett. 8(1), 1–4 (2023)
70. Codău, C., Buta, R.-C., Păstrăv, A., Dolea, P., Palade, T., Puschita, E.: Experimental evaluation of an SDR-based UAV localization system. Sensors 24(9), 2789 (2024)
71. Fisher, D., Lukow, S., Berezutskiy, G., Gil, I., Levy, T., Zeiri, Y.: Machine learning improves trace explosive selectivity: application to nitrate-based explosives. J. Phys. Chem. A 124(46), 1089–5639 (2020)
72. RDTECH Group: Cutting-edge software defined radios (SDRs) & Datalink solutions for UAVs & unmanned systems. https://www.unmannedsystemstechnology.com/company/rdtech-group/ (2024). Accessed 8 Apr 2024
73. Ajakwe, S.O., Ihekoronye, V.U., Kim, D.-S., Lee, J.M.: Pervasive intrusion detection scheme to mitigate sensor attacks on uav networks. In: 2022 Korean Institute of Communication and Sciences Summer Conference, pp. 1267–1268. Korea Institute Of Communication Sciences, Daejeon (2022)
74. Tropea, M., Spina, M.G., Lakas, A., Sarigiannidis, P., Rango, F.D.: SecG-PSR: a secure GPSR protocol for FANET against Sybil and Gray Hole attacks. IEEE Access (2024). https://doi.org/10.1109/ACCESS.2024.3433512
75. Sachdeva, H., Gupta, S., Misra, A., Chauhan, K., Dave, M.: Privacy and security improvement in UAV network using blockchain. Int. J. Commun. Networks Distrib. Syst. 29(4), 383–406 (2023)
76. Ge, C., Ma, X., Liu, Z.: A semi-autonomous distributed blockchain-based framework for UAVs system. J. Syst. Archit. 107, 101728 (2020)
77. Maxa, J.-A., Mahmoud, M.-S.B., Larrieu, N.: Survey on UAANET routing protocols and network security challenges. In: Ad Hoc Sens. Wireless Networks, pp. 231–320. IEEE, Piscataway, NJ (2017)
78. Ceviz, O., Sadioglu, P., Sen, S.: Analysis of routing attacks in FANETs. In: International Conference on Ad Hoc Networks, pp. 3–17. Springer, Cham (2021)
79. Daniel, A., et al.: A survey on detection of clones in wireless sensor networks. Int. J. Comput. Appl. 91(7), 48–52 (2014)
80. Xiong, R., Xiong, L., Shan, F., Luo, J.: SBHA: an undetectable black hole attack on UANET in the sky. Concurrency Comput.: Pract. Exp. 35(13), e6700 (2023)
81. Sharma, J., Mehra, P.S.: Secure communication in IoT-based UAV networks: a systematic survey. Internet Things 23, 100883 (2023)
82. Pramitarini, Y., Perdana, R.H.Y., Shim, K., An, B.: DLSMR: deep learning-based secure multicast routing protocol against wormhole attack in flying ad hoc networks with cell-free massive multiple-input multiple-output. Sensors 23(18), 7960 (2023)
83. Schweitzer, N., Dvir, A., Stulman, A.: Network wormhole attacks without a traditional wormhole. Ad Hoc Networks 151, 103286 (2023)
84. Airlangga, G., Liu, A.: A study of the data security attack and defense pattern in a centralized UAV–cloud architecture. Drones 7(5), 289 (2023)
85. Wani, A.R., Gupta, S.K., Khanam, Z., Rashid, M., Alshamrani, S.S., Baz, M.: A novel approach for securing data against adversary attacks in UAV embedded HetNet using identity based authentication scheme. IET Intell. Transp. Syst. 17(11), 2171–2189 (2023)
86. Seo, S., Lee, Y., Lee, S., Oh, S., Son, J.: Replay attack based neutralization method for DJI UAV detection/identification systems. J. Aerosp. Syst. Eng. 17(4), 133–143 (2023)
87. Bekmezci, İ., Şentürk, E., Türker, T.: Security issues in flying ad-hoc networks (FANETs). J. Aeronaut. Space Technol. 9(2), 13–21 (2016)
88. Wu, B., Chen, J., Wu, J., Cardei, M.: A survey of attacks and countermeasures in mobile ad hoc networks. Wireless Network Secur. 103–135 (2007)
89. Zhi, Y., Fu, Z., Sun, X., Yu, J.: Security and privacy issues of UAV: a survey. Mobile Networks Appl. 25(1), 95–101 (2020)
90. Tlili, F., Fourati, L.C., Ayed, S., Ouni, B.: Investigation on vulnerabilities, threats and attacks prohibiting UAVs charging and depleting UAVs batteries: assessments & countermeasures. Ad Hoc Networks 129, 102805 (2022)
91. Pu, C., Zhu, P.: Defending against flooding attacks in the internet of drones environment. In: 2021 IEEE Global Communications Conference (GLOBECOM), pp. 1–6. IEEE, Piscataway, NJ (2021)
92. Amponis, G., Radoglou-Grammatikis, P., Lagkas, T., Mallouli, W., Cavalli, A., Klonidis, D., Markakis, E., Sarigiannidis, P.: Threatening the 5G core via PFCP DoS attacks: the case of blocking UAV communications. EURASIP J. Wireless Commun. Networking 2022(1), 124 (2022)
93. Obaidat, M.S., Woungang, I., Dhurandher, S.K., Koo, V.: Preventing packet dropping and message tampering attacks on AODV-based mobile ad hoc networks. In: 2012 International Conference on Computer, Information and Telecommunication Systems (CITS), pp. 1–5. IEEE, Piscataway, NJ (2012)
94. Kadripathi, K., Ragav, L.Y., Shubha, K., Chowdary, P.H.: De-authentication attacks on rogue UAVs. In: 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), pp. 1178–1182. IEEE, Piscataway, NJ (2020)
95. Jan, S.U., Qayum, F., Khan, H.U.: Design and analysis of lightweight authentication protocol for securing IoD. IEEE Access 9, 69 287–69 306 (2021)
96. Sedjelmaci, H., Senouci, S.M.: Cyber security methods for aerial vehicle networks: taxonomy, challenges and solution. J. Supercomput. 74(10), 4928–4944 (2018)
97. Mpitziopoulos, A., Gavalas, D., Konstantopoulos, C., Pantziou, G.: A survey on jamming attacks and countermeasures in WSNs. IEEE Commun. Surv. Tut. 11(4), 42–56 (2009)
98. Deebak, B.D., Hwang, S.O.: Intelligent drone-assisted robust lightweight multi-factor authentication for military zone surveillance in the 6G era. Comput. Networks 225, 109664 (2023)
99. Vajravelu, A., Kumar, N.A., Sarkar, S., Degadwala, S.: Security threats of unmanned aerial vehicles. In: Wireless Networks: Cyber Security Threats and Countermeasures, pp. 133–164. Springer, Cham (2023)
100. Khan, Z.A.: Cyber security analysis of UAVs in emergency medical services. Master Thesis, Linköping University (2023)
101. Desnitsky, V., Kotenko, I.: Simulation and assessment of battery depletion attacks on unmanned aerial vehicles for crisis management infrastructures. Simul. Modell. Pract. Theory 107, 102244 (2021)
102. Shakhov, V., Koo, I.: Depletion-of-battery attack: specificity, modelling and analysis. Sensors 18(6), 1849 (2018)
103. Lopez, A.B., Vatanparvar, K., Nath, A.P.D., Yang, S., Bhunia, S., Faruque, M.A.A.: A security perspective on battery systems of the Internet of Things. J. Hardware Syst. Secur. 1, 188–199 (2017)
104. Chen, J., Feng, Z., Wen, J.-Y., Liu, B., Sha, L.: A container-based DoS attack-resilient control framework for real-time UAV systems. In: 2019 Design, Automation & Test in Europe Conference & Exhibition (DATE), pp. 1222–1227. IEEE, Piscataway, NJ (2019)
105. Vasconcelos, G., Carrijo, G., Miani, R., Souza, J., Guizilini, V.: The impact of DoS attacks on the AR. drone 2.0. In: 2016 XIII Latin

American Robotics Symposium and IV Brazilian Robotics Symposium (LARS/SBR), pp. 127–132. IEEE, Piscataway, NJ (2016)
106. Vasconcelos, G., Miani, R.S., Guizilini, V.C., Souza, J.R.: Evaluation of DoS attacks on commercial Wi-Fi-based UAVs. Int. J. Commun. Networks Inf. Secur. 11(1), 212–223 (2019)
107. Guin, U., Huang, K., DiMase, D., Carulli, J.M., Tehranipoor, M., Makris, Y.: Counterfeit integrated circuits: a rising threat in the global semiconductor supply chain. Proc. IEEE 102(8), 1207–1228 (2014)
108. Belikovetsky, S., Yampolskiy, M., Toh, J., Gatlin, J., Elovici, Y.: dr0wned–cyber-physical attack with additive manufacturing. In: 11th USENIX workshop on offensive technologies (WOOT 17), p. 1. ACM, New York, NY (2017)
109. Spreitzer, R., Moonsamy, V., Korak, T., Mangard, S.: Systematic classification of side-channel attacks: a case study for mobile devices. IEEE Commun. Surv. Tut. 20(1), 465–488 (2017)
110. Mansfield, K., Eveleigh, T., Holzer, T.H., Sarkani, S.: Unmanned aerial vehicle smart device ground control station cyber security threat model. In: 2013 IEEE International Conference on Technologies for Homeland Security (HST), pp. 722–728. IEEE, Piscataway, NJ (2013)
111. Ciancioso, R., Budhwa, D., Hayajneh, T.: A framework for zero day exploit detection and containment. In: 2017 IEEE 15th International Conference on Dependable, Autonomic and Secure Computing, 15th International Conference on Pervasive Intelligence and Computing, 3rd International Conference on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech), pp. 663–668. IEEE, Piscataway, NJ (2017)
112. Al-Rushdan, H., Shurman, M., Alnabelsi, S.H., Althebyan, Q.: Zero-day attack detection and prevention in software-defined networks. In: 2019 International Arab Conference on Information Technology (ACIT), pp. 278–282. IEEE, Piscataway, NJ (2019)
113. Saputro, J.A., Hartadi, E.E., Syahral, M.: Implementation of gps attacks on DJI Phantom 3 standard drone as a security vulnerability test. In: 2020 1st International Conference on Information Technology, Advanced Mechanical and Electrical Engineering (ICITAMEE), pp. 95–100. IEEE, Piscataway, NJ (2020)
114. Feng, Z., Guan, N., Lv, M., Liu, W., Deng, Q., Liu, X., Yi, W.: Efficient drone hijacking detection using two-step GA-XGBoost. J. Syst. Archit. 103, 101694 (2020)
115. Tan, Y., Wang, J., Liu, J., Kato, N.: Blockchain-assisted distributed and lightweight authentication service for industrial unmanned aerial vehicles. IEEE Internet Things J. 9(18), 16 928–16 940 (2022)
116. Ajakwe, S.O., Saviour, I.I., Kim, J.-H., Kim, D.-S., Lee, J.M.: BANDA: a novel blockchain-assisted network for drone authentication. In: 2023 Fourteenth International Conference on Ubiquitous and Future Networks (ICUFN), pp. 120–125. IEEE, Piscataway, NJ (2023)
117. Saraswat, D., Verma, A., Bhattacharya, P., Tanwar, S., Sharma, G., Bokoro, P.N., Sharma, R.: Blockchain-based federated learning in UAVs beyond 5G networks: a solution taxonomy and future directions. IEEE Access 10, 33 154–33 182 (2022)
118. Pu, C., Li, Y.: Lightweight authentication protocol for unmanned aerial vehicles using physical unclonable function and chaotic system. In: 2020 IEEE International Symposium on Local and Metropolitan Area Networks LANMAN, pp. 1–6. IEEE, Piscataway, NJ (2020)
119. Maeng, S.J., Yapıcı, Y., Güvenç, İ., Bhuyan, A., Dai, H.: Precoder design for physical-layer security and authentication in massive MIMO UAV communications. IEEE Trans. Veh. Technol. 71(3), 2949–2964 (2022)
120. Fu, H., Sheng, Z., Nasir, A.A., Muqaibel, A.H., Hanzo, L.: Securing the UAV-aided non-orthogonal downlink in the face of colluding eavesdroppers. IEEE Trans. Veh. Technol. 71(6), 6837–6842 (2022)
121. Ajakwe, S.O., Ihekoronye, V.U., Kim, D.-S., Lee, J.-M.: SimNet: UAV-integrated sensor nodes localization for communication intelligence in 6G networks. In: 2022 27th Asia Pacific Conference on Communications (APCC), pp. 344–347. IEEE, Piscataway, NJ (2022)
122. Davidson, D., Wu, H., Jellinek, R., Singh, V., Ristenpart, T.: Controlling UAVs with sensor input spoofing attacks. In: 10th USENIX workshop on offensive technologies (WOOT 16), pp. 221–231. ACM, New York, NY (2016)
123. Ihekoronye, V.U., Ajakwe, S.O., Kim, D.-S., Lee, J.M.: Hierarchical intrusion detection system for secured military drone network: a perspicacious approach. In: MILCOM 2022-2022 IEEE Military Communications Conference (MILCOM), pp. 336–341. IEEE, Piscataway, NJ (2022)
124. Silva, L.M.D., Ferrão, I.G., Dezan, C., Espes, D., Branco, K.R.: Anomaly-based intrusion detection system for in-flight and network security in UAV swarm. In: 2023 International Conference on Unmanned Aircraft Systems (ICUAS), pp. 812–819. IEEE, Piscataway, NJ (2023)
125. Ajakwe, S., Ihekoronye, V.U., Kim, D., Lee, J.-M.: Pervasive intrusion detection scheme to mitigate sensor attacks on UAV networks. In: 2022 Korean Institute of Communication and Sciences Summer Conference, pp. 1267–1268. Korean Institutes of Communications and Information Sciences, Seoul (2022)
126. Abro, G.E.M., Zulkifli, S.A.B., Masood, R.J., Asirvadam, V.S., Laouti, A.: Comprehensive review of UAV detection, security, and communication advancements to prevent threats. Drones 6(10), 284 (2022)
127. Yu, S., Lee, J., Sutrala, A.K., Das, A.K., Park, Y.: LAKA-UAV: Lightweight authentication and key agreement scheme for cloud-assisted unmanned aerial vehicle using blockchain in flying ad-hoc networks. Comput. Networks 224, 109612 (2023)
128. Mallikarachchi, D., Wong, K., Lim, J.M.-Y.: An authentication scheme for FANET packet payload using data hiding. J. Inf. Secur. Appl. 77, 103559 (2023)
129. Hussain, S., Mahmood, K., Khan, M.K., Chen, C.-M., Alzahrani, B.A., Chaudhry, S.A.: Designing secure and lightweight user access to drone for smart city surveillance. Comput. Stand. Interfaces 80, 103566 (2022)
130. Mowla, N.I., Tran, N.H., Doh, I., Chae, K.: Afrl: Adaptive federated reinforcement learning for intelligent jamming defense in FANET. J. Commun. Networks 22(3), 244–258 (2020)
131. Puñal, O., Pereira, C., Aguiar, A., Gross, J.: Crawdad dataset uportorwthaachen/vanetjamming2014 (v. 2014-05-12) (2014). https://ieee-dataport.org/open-access/crawdad-uportorwthaachenvanetjamming2014. Accessed 14 Apr 2024
132. Bouhamed, O., Bouachir, O., Aloqaily, M., Ridhawi, I.A.: Lightweight IDs for UAV networks: a periodic deep reinforcement learning-based approach. In: 2021 IFIP/IEEE International Symposium on Integrated Network Management (IM), pp. 1032–1037. IEEE, Piscataway, NJ (2021)
133. Ramadan, R.A., Emara, A.-H., Al-Sarem, M., Elhamahmy, M.: Internet of drones intrusion detection using deep learning. Electronics 10(21), 2633 (2021)
134. Titouna, C., Naït-Abdesselam, F.: Securing unmanned aerial systems using mobile agents and artificial neural networks. In: 2021 International Wireless Communications and Mobile Computing (IWCMC), pp. 825–830. IEEE, Piscataway, NJ (2021)
135. Chulerttiyawong, D., Jamalipour, A.: Sybil attack detection in internet of flying things-IoFT: a machine learning approach. IEEE Internet Things J. 10(14), 12854–12866 (2023)
136. Nayfeh, M., Li, Y., Shamaileh, K.A., Devabhaktuni, V., Kaabouch, N.: Machine learning modeling of GPS features with applications to UAV location spoofing detection and classification. Comput. Secur. 126, 103085 (2023)
137. Shrestha, R., Omidkar, A., Roudi, S.A., Abbas, R., Kim, S.: Machine-learning-enabled intrusion detection system for cellular connected UAV networks. Electronics 10(13), 1549 (2021)
138. Whelan, J., Sangarapillai, T., Minawi, O., Almehmadi, A., El-Khatib, K.: Novelty-based intrusion detection of sensor attacks on unmanned aerial vehicles. In: Proceedings of the 16th ACM Symposium on QoS and Security for Wireless and Mobile Networks, pp. 23–28. ACM, New York, NY (2020)
139. Sedjelmaci, H., Senouci, S.M., Ansari, N.: A hierarchical detection and response system to enhance security against lethal cyber-attacks in UAV networks. IEEE Trans. Syst. Man Cybern. Syst. 48(9), 1594–1606 (2017)
140. Dantu, S., Yadav, R.D., Rachakonda, A., Roy, S., Baldi, S.: Adaptive anti-swing control for clasping operations in quadrotors with cable-suspended payload. In: 2023 62nd IEEE Conference on Decision and Control (CDC), pp. 503–508. IEEE, Piscataway, NJ (2023)

141. Jin, X., Hu, Z.: Attacker-resilient adaptive path following of a quadrotor with environment-aware dynamic constraints. IEEE Trans. Aerosp. Electron. Syst. 59(6), 7822–7834 (2023)
142. Ames, A.D., Xu, X., Grizzle, J.W., Tabuada, P.: Control barrier function based quadratic programs for safety critical systems. IEEE Trans. Autom. Control 62(8), 3861–3876 (2016)
143. Jin, X., Dai, S.-L., Liang, J.: Fixed-time path-following control of an autonomous vehicle with path-dependent performance and feasibility constraints. IEEE Trans. Intell. Veh. 8(1), 458–468 (2021)
144. Amjad, B., Ahmed, Q.Z., Lazaridis, P.I., Hafeez, M., Khan, F.A., Zaharis, Z.D.: Radio SLAM: a review on radio-based simultaneous localization and mapping. IEEE Access 11, 9260–9278 (2023)
145. Yang, L., Ye, J., Zhang, Y., Wang, L., Qiu, C.: A semantic slam-based method for navigation and landing of UAVs in indoor environments. Knowl.-Based Syst. 293, 111693 (2024)
146. Ghaseminajm, F., Alsamdi, M., Ikki, S.S.: Error bounds for localization in mmWave MIMO systems: effects of hardware impairments considering perfect and imperfect clock synchronization. IEEE Syst. J. 16(4), 6350–6359 (2022)
147. Liu, D., Wu, J., Du, Y., Zhang, R., Cong, M.: SBC-SLAM: semantic bio-inspired collaborative slam for large-scale environment perception of heterogeneous systems. IEEE Trans. Instrum. Meas. (2024)
148. Friess, C., Niculescu, V., Polonelli, T., Magno, M., Benini, L.: Fully onboard SLAM for distributed mapping with a swarm of nano-drones. IEEE Internet Things J. 11(20), 32363–32380 (2024). https://doi.org/10.1109/JIOT.2024.3367451
149. Ou, B., Liu, F., Niu, G.: Distributed localization for UAV-UGV cooperative systems using information consensus filter. Drones 8(4), 166 (2024)
150. Wang, W., You, M., Sun, L., Zhang, X., Zong, Q.: Intelligent cooperative exploration path planning for UAV swarm in an unknown environment. Chin. J. Eng. 46(7), 1197–1206 (2024)
151. Zhou, H., Yao, Z., Lu, M.: Lidar/UWB fusion based slam with anti-degeneration capability. IEEE Trans. Veh. Technol. 70(1), 820–830 (2020)
152. Song, Y., Guan, M., Tay, W.P., Law, C.L., Wen, C.: UWB/Lidar fusion for cooperative range-only SLAM. In: 2019 International Conference on Robotics and Automation (ICRA), pp. 6568–6574. IEEE, Piscataway, NJ (2019)
153. Liu, D., Wu, J., Du, Y., Zhang, R., Cong, M.: SBC-SLAM: semantic bioinspired collaborative SLAM for large-scale environment perception of heterogeneous systems. IEEE Trans. Instrum. Meas. 73, 1–10 (2024)
154. Wang, R., Deng, Z.: Co-operatively increasing smoothing and mapping based on switching function. Appl. Sci. 14(4), 1543 (2024)
155. Fernandez-Cortizas, M., Bavle, H., Perez-Saura, D., Sanchez-Lopez, J.L., Campoy, P., Voos, H.: Multi S-graphs: an efficient distributed semantic-relational collaborative slam. IEEE Rob. Autom. Lett. 9(6), 6004–6011 (2024)
156. Liu, Y., Yao, W., Zhou, D., Wu, L., You, S., Liu, H., Zhan, L., Zhao, J., Lu, H., Gao, W., et al.: Recent developments of FNET/GridEye—a situational awareness tool for smart grid. CSEE J. Power Energy Syst. 2(3), 19–27 (2016)
157. Lei, W., Wen, H., Wu, J., Hou, W.: MADDPG-based security situational awareness for smart grid with intelligent edge. Appl. Sci. 11(7), 3101 (2021)
158. Wang, W., Guo, K., Cao, W., Zhu, H., Nan, J., Yu, L.: Review of electrical and electronic architectures for autonomous vehicles: topologies, networking and simulators. Autom. Innovation 7(1), 82–101 (2024)
159. Haque, E., Hasan, K., Ahmed, I., Alam, M.S., Islam, T.: Enhancing UAV security through zero trust architecture: an advanced deep learning and explainable ai analysis. arXiv:2403.17093 (2024)
160. Nkoro, E.C., Njoku, J.N., Nwakanma, C.I., Lee, J.-M., Kim, D.-S.: Zero-trust marine cyberdefense for IoT-based communications: an explainable approach. Electronics 13(2), 276 (2024)
161. Ajakwe, S.O., Deji-Oloruntoba, O., Olatunbosun, S.O., Duorinaah, F.X., Bayode, I.A.: Multidimensional perspective to data preprocessing for model cognition verity: data preparation and cleansing-approaches for model optimal feedback validation. In: Recent Trends and Future Direction for Data Analytics, pp. 15–57. IGI Global, Hershey, PA (2024)
162. Ajakwe, S.O., Ihekoronye, V.U., Kim, D.-S., Lee, J.M.: AI-trust in intelligent autonomous decision-centric systems: introspection of security architectures. In: Proceedings of the Korean Institute of Communications Society (KICS) Fall Conference 2022, pp. 1–2. Korean Institute of Communications Society, Seoul (2022)
163. Markets and Markets. Explaianble AI Markets. https://www.marketsandmarkets.com/Market-Reports/explainable-ai-market-47650132.html (2024). Accessed 3 May 2024
164. Artificial intelligence risk management framework. https://airc.nist.gov/AIRMFKnowledgeBase/Playbook (2023). Accessed 3 May 2024
165. Zhang, J., Zhong, S., Wang, T., Chao, H.-C., Wang, J.: Blockchain-based systems and applications: a survey. J. Internet Technol. 21(1), 1–14 (2020)
166. Alqarni, M.A.: Secure UAV adhoc network with blockchain technology. Plos one 19(5), e0302513 (2024)
167. Liu, Y., Gao, J., Lu, Y., Cao, R., Yao, L., Xia, Y., Han, D.: Lightweight blockchain-enabled secure data sharing in dynamic and resource-limited UAV networks. IEEE Network 38(4), 25–31 (2024)
168. Chen, C.-L., Deng, Y.-Y., Zhu, S., Tsaur, W.-J., Weng, W.: An IoT and blockchain based logistics application of UAV. Multimedia Tools Appl. 83(1), 655–684 (2024)
169. Wang, H., Wang, C., Zhou, K., Liu, D., Zhang, X., Cheng, H.: TEBChain: a trusted and efficient blockchain-based data sharing scheme in UAV-assisted IoV for disaster rescue. IEEE Trans. Network Serv. Manage. 21(4), 4119–4130 (2024)
170. Chen, L., Zhu, Y., Liu, S., Yu, H., Zhang, B.: PUF-based dynamic secret-key strategy with hierarchical blockchain for UAV swarm authentication. Comput. Commun. 218, 31–43 (2024)
171. Hafeez, S., Shawky, M.A., Al-Quraan, M., Mohjazi, L., Imran, M.A., Sun, Y.: Beta-UAV: blockchain-based efficient authentication for secure UAV communication. arXiv:2402.15817 (2024)
172. Li, Z., Chen, Q., Li, J., Huang, J., Mo, W., Wong, D.S., Jiang, H.: A secure and efficient UAV network defense strategy: Convergence of blockchain and deep learning. Comput. Stand. Interfaces 90, 103844 (2024)
173. Hafeez, S., Cheng, R., Mohjazi, L., Sun, Y., Imran, M.A.: Blockchain-enhanced UAV networks for post-disaster communication: a decentralized flocking approach. arXiv:2403.04796 (2024)
174. Xie, H., Zheng, J., Wei, S., Hu, C.: Blockchain-and-6G-based ubiquitous UAV task security management architecture. Comput. Commun. 217, 259–267 (2024)
175. Stafford, V.: Zero trust architecture. NIST Spec. Publ. 800, 207 (2020)
176. Hasan, S., Amundson, I., Hardin, D.: Zero trust architecture patterns for cyber-physical systems. SAE Int. J. Adv. Curr. Pract. Mobility 5, 1919–1931 (2023)
177. Yang, D., Zhao, Y., Wu, K., Guo, X., Peng, H.: An efficient authentication scheme based on zero trust for UAV swarm. In: 2021 International Conference on Networking and Network Applications (NaNA), pp. 356–360. IEEE, Piscataway, NJ (2021)
178. Dong, C., Jiang, F., Chen, S., Liu, X.: Continuous authentication for UAV delivery systems under zero-trust security framework. In: 2022 IEEE International Conference on Edge Computing and Communications (EDGE), pp. 123–132. IEEE, Piscataway, NJ (2022)
179. Sedjelmaci, H., Ansari, N.: Zero trust architecture empowered attack detection framework to secure 6G edge computing. IEEE Network 38(1), 196–202 (2023)

How to cite this article: Ajakwe, S.O., Kim, D.-S.: Facets of security and safety problems and paradigms for smart aerial mobility and intelligent logistics. IET Intell. Transp. Syst. 18(Suppl. 1), 2827–2855 (2024). https://doi.org/10.1049/itr2.12579