ORIGINAL RESEARCH Open access

Large Language Models for Collaborative Control and Security Optimization in UAV Clusters

William Taylor[1*], Emily Davis[1], Thomas Wilson[2], Daniel Carter[3]

Abstract

As unmanned aerial vehicle (UAV) capabilities progress, multi-unit cooperative missions have become the fundamental model for boosting operational performance. Yet, expansive UAV swarms encounter hurdles such as shifting security vulnerabilities, difficulties in merging disparate data sources, and decision delays driven by constrained resources. Traditional single-unit intelligent designs exhibit weaknesses when confronting novel dangers, notably a lack of immediate response proficiency. To resolve these problems, this work puts forward an LLM-layered collaborative security architecture (LLM-LCSA) for multi-unit cooperative protection. The design refines the spatiotemporal integration efficiency of multisource asynchronous information through cloud–edge–end cooperative distribution, blending a lightweight LLM on the terminal, a medium-scale LLM at the edge, and a foundational LLM in the cloud. Moreover, a Mixture of Experts (MoE) intelligent algorithm that selectively triggers the most suitable expert modules by tapping into a threat–expert correlation matrix is introduced, improving the precision of intricate threat detection while maintaining dynamic flexibility. A resource-cognizant multi-objective optimization formulation is also built to derive optimal choices within resource boundaries. Simulation findings reveal that, compared with conventional techniques, LLM-LCSA yields a mean 7.92% gain in threat identification accuracy, slashes the system's overall response interval by 44.52%, and facilitates resource allocation during low-demand windows. This framework provides a streamlined, intelligent, and expandable solution for secure collaboration across UAV collectives. Subsequent investigations should delve deeper into its applicability within 6G network convergence and extensive swarm conditions.

Keywords Large language models, Unmanned aerial vehicle, Security, Cluster control

*Correspondence:
William Taylor
william.taylor@auckland.ac.nz
[1] Department of AI for Kiwifruit and Apple Orchard Management, School of Agriculture, University of Auckland, Auckland, New Zealand
[2] Department of Hyperspectral Imaging for Fruit Ripeness Prediction, School of Agriculture, University of Otago, Dunedin, New Zealand
[3] Department of Smart Pollination and Bee Activity Monitoring, School of Agriculture, Massey University, Palmerston North, New Zealand

Introduction

Motivation

Given the widespread adoption of unmanned aerial vehicle (UAV) technology across critical fields, including disaster response [1], agricultural plant protection [2], power inspection [3], and logistics and distribution [4], coordinating multiple UAVs has become a central tactic for improving mission outcomes. As networked communication systems steadily

This is an open access article distributed under the terms of the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License (CC BY-NC-SA 4.0), which permits non-commercial use, distribution, reproduction, and adaptation in any medium or format, provided that appropriate credit is given to the original author(s) and source, a link to the license is provided, and any changes made are indicated. Adapted material must be distributed under the same license.

© 2023 The Author(s). | Published by Agro Intelligence Research Press

mature, the number of UAVs that can be managed within a swarm is likewise growing. Compared with smaller-scale formations, large UAV swarms can carry heavier payloads, substantially widening their operational reach.

While swarming improves scalability, it also introduces systemic challenges such as proliferating dynamic security risks, inefficient cross-platform teamwork, and decision delays rooted in resource scarcity [5]. Traditional single-unit intelligent structures hit limits when exposed to emerging threats, for instance, GPS spoofing [6], cooperative network assaults [7], and sensor jamming blends, alongside struggles with merging multisource streams, poor real-time reaction speed [8], and sluggish adaptive defense, all of which gravely undermine the safety and dependability of UAV swarms within complex environments. When a UAV swarm experiences a cyber intrusion, the coordinated motion of the entire collective is disrupted, severely endangering safety. Lately, a growing number of researchers have focused on ensuring secure, synchronized flight among swarming craft under cyberattack scenarios.

State of the art

Cooperative regulation of UAV swarms can be classified into centralized, decentralized, and distributed control paradigms [9]. Centralized methods can achieve globally optimal control, yet drawbacks such as high communication overhead and fragile formation stability limit the expandability of drone swarms. Distributed strategies rely solely on local information sharing to harmonize the group, reducing communication bandwidth requirements while preserving robust fault tolerance and growth potential. Decentralized strategies forgo a central coordinator and can achieve only local optimality; nevertheless, they offer benefits such as modular design and swarm extensibility. Beyond these overarching frameworks, investigators have delved into swarm protection.

Raja *et al.* [10] introduced an innovative multilayer blockchain-aided 6G Internet of Drones (MLB-IoD) ecosystem that enhances system resilience against attacks while enabling efficient route planning through safeguards and compliance protocols. Karmakar *et al.* [11] engineered a blockchain-based distributed authentication scheme for drone swarms. Blockchain enables drone identity data to reside in tamper-proof storage, while companion smart contracts provide a convenient access governance model. Jangsher *et al.* [12] advanced an efficient group secret key (GSK) protocol for protected communication inside distributed drone swarms. The suggested protocol harnesses network coding to craft cooperative signals sent through the channel, signals that stand apart from the derived keys. This presented a remedy to uphold secure authentication for drone collectives. Viana *et al.* [13] developed a deep learning framework to detect attack patterns in UAV communications under 5G conditions. The framework can reliably flag attack behaviors in both line-of-sight (LoS) and non-line-of-sight (NLoS) settings, as well as in random mixes of both, thereby enhancing the protection and reliability of UAV swarms amid interference and complex communication landscapes. Lopez *et al.* [14] proposed a security design for wireless mesh networks in UAV swarm exchanges, deeply analyzed weaknesses and threats spanning the physical tier to the application tier, and outlined corresponding defense measures.

Because legacy UAV safety governance systems ordinarily rely on fixed rules and heuristics, these approaches stumble in fluid environments and exhibit limited safety decision flexibility and coordination efficacy due to the difficulty of detecting complex and shifting threats [15, 16]. The integration of large language models (LLMs) into UAV swarm safety addresses gaps left by older methods in areas such as adaptation to changing settings [17], coordinated intelligent decision-making [18], resource allocation [19], and overall system robustness. **Figure 1** portrays a UAV swarm within an intelligent control cooperation setting. Tiered backing from terminal-, edge-, and cloud-level LLMs amplifies the swarm's autonomous sensing, comprehension, and decision-making, equipping it to adapt more nimbly to varied application contexts.

© 2023 The Author(s). | Published by Agro Intelligence Research Press

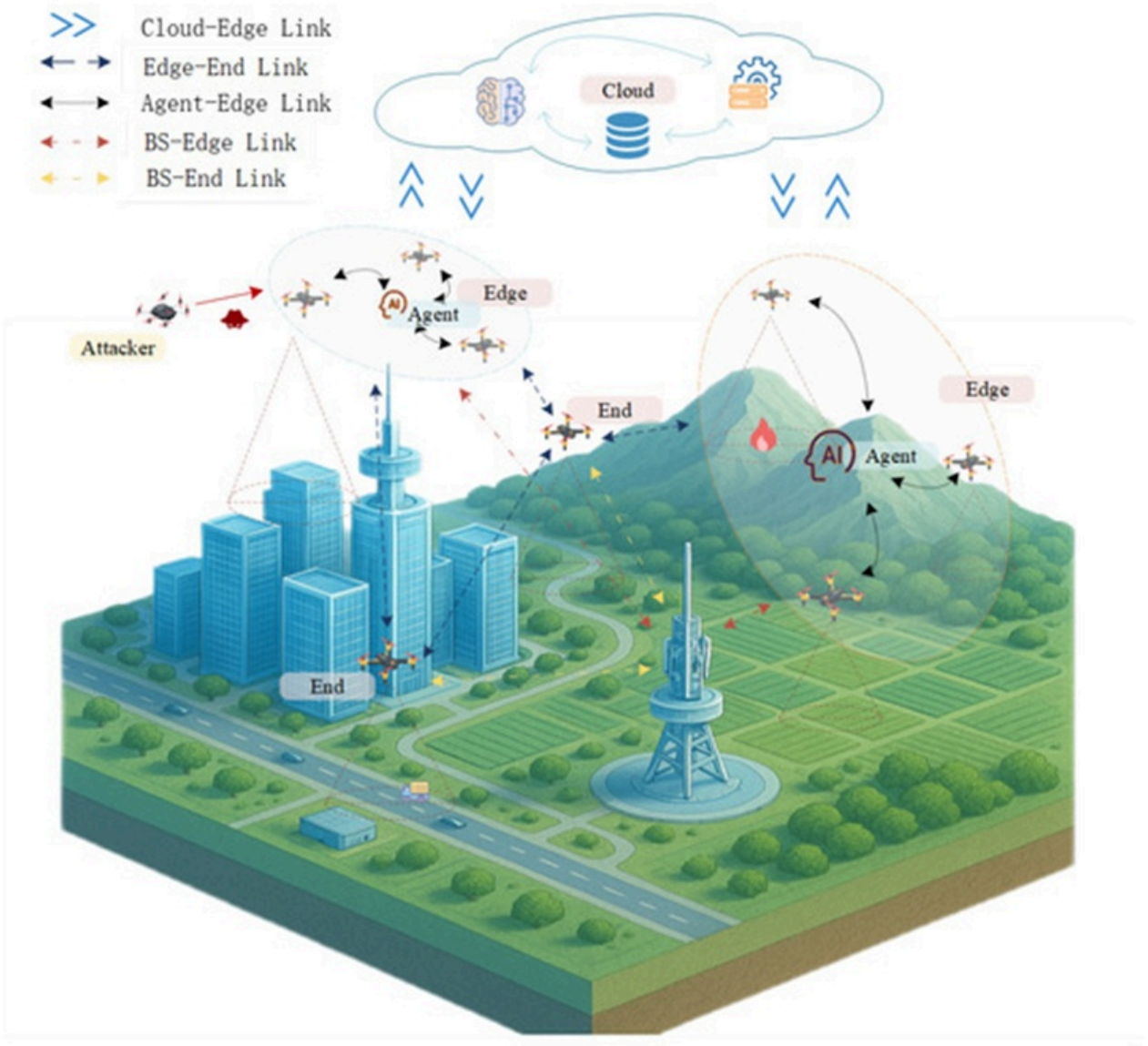


Figure 1. Intelligent collaboration of UAV clusters.

Comparison of related work

Prior work has demonstrated real-world viability. Aikins *et al.* [20] presented a case study demonstrating LLM support for up to 1000 drones flying in concert, highlighting the potential of LLMs to steer large-scale swarm operations. Li *et al.* [21] proposed refining UAV positioning and power regulation using LLMs to enhance swarm anti-jamming capabilities in crisis communication contexts and preserve link stability and integrity. Han *et al.* [22] unveiled CoLLM, a distributed LLM cooperative inference framework designed for infrastructure-free settings to prevent the spillage of smart decisions if a single node is compromised. Zhu *et al.* [23] described a Transformer-based UAV path-planning routine that rapidly crafts optimal routes, mitigates data transfer and processing lag, and reduces the risk of data corruption or staleness, offering an effective solution for safe data harvesting by UAV swarms in complex terrain [23]. Yang *et al.* [17] conducted an extensive survey of LLM deployments for UAV safety. They observed that LLMs can meaningfully sharpen threat sensing and reaction capabilities within UAV swarms under complex conditions via multimodal data fusion and on-the-fly decision-making, thereby considerably boosting swarm security. Emami *et al.* [24] proposed an In-Context Learning (ICL) data-

© 2023 The Author(s). | Published by Agro Intelligence Research Press

gathering orchestration framework based on LLMs, which shines in trials against jailbreak attacks, thus preserving communication safety.

Additionally, certain scholars have combined LLMs with other technologies to enable more productive and secure cooperative command of UAV swarms. Golam *et al.* [25] wove LLMs into a blockchain fabric to enable online detection of emerging and intricate threats in UAV traffic without additional training cycles. Drawing on the context-grasping capabilities of LLMs, they performed semantic-tier anomaly detection on immutable UAV traffic logs stored on the blockchain, sharply reducing both false alarm and miss rates. Piggott *et al.* [26] advanced an adversarial chatbot anchored in LLMs that interprets network protocols and stages man-in-the-middle strikes on links between UAVs and ground control stations (GCSs), auto-crafting fake network packets. This route can be further mined to harden UAV swarm robustness against intrusions. Sezgin [27] also significantly improved the security decision-making capabilities of UAV swarms in harsh environments by combining LLMs with RAG technology. Javaid *et al.* [18] dissected the protective use cases of LLMs in UAV swarms; spelled out their pivotal function in menace spotting, order verification, and crisis handling; and laid out an LLM-propelled spectrum sensing and sharing technique able to locate jamming sources on the fly and fluidly hop channels to shield swarm links from suppression or trickery. Zhou *et al.* [28] combined large language models with Q-learning to effectively address safety concerns in UAV swarm decision-making, orchestration, and fine-tuning in uncharted spaces.

Table 1 summarizes investigative approaches for UAV swarm protection. Even so, present-day LLM frameworks for UAV swarm security still run into a host of obstacles in multi-craft cooperative safety contexts, as summarized in **Table 2**. Thus, a void persists for an adaptive, resource-attentive collaborative safeguarding scaffold capable of juggling multisource inputs, fluid threat postures, and resource-strapped circumstances within large UAV swarms. Current answers tend to focus on separate components such as authentication, breach detection, or path design, without knitting them into an integrated, tiered decision-making architecture that bridges the cloud, edge, and terminal nodes.

Table 1. Categorized summary of research methods in UAV cluster security.

Field	Technical category	Ref.	Year	Technical approach	Key innovation/Strength
Traditional method	Cryptography	[29]	2022	Introduced a lightweight challenge–response authentication scheme utilizing elliptic curve cryptography.	It is well-suited for SDN-enabled UAV systems because of its low computational complexity.
		[12]	2023	Presented an efficient GSK protocol called the sequential secret group key algorithm for distributed UAV networks.	Achieved dependable GSK generation while balancing transmission overhead and communication reliability.
	Multilayer Model	[30]	2023	Developed a multilayer graph network model for consensus control in large-scale UAV swarms.	Enhanced the scalability and resilience of extensive UAV cluster topologies.
		[10]	2025	Proposed a multilayer blockchain-supported 6G drone internet framework (MLB-IoD).	Delivered strong protection against attacks through authentication and encryption mechanisms.
	Blockchain	[11]	2024	Designed a blockchain-enabled distributed identity	Improved drone swarm network efficiency while ensuring reliable communication.

© 2023 The Author(s). | Published by Agro Intelligence Research Press

				authentication mechanism for UAV swarms.	
	Threat Identification	[14]	2021	Proposed a wireless mesh network security framework and evaluated vulnerabilities from the physical layer through the application layer.	Offered end-to-end security protection for UAV swarm communications.
		[31]	2024	Built a UAV swarm intrusion detection framework based on time probability automata (TPA).	Capable of adapting to emerging attack behaviors and detecting zero-day threats.
		[13]	2024	Developed a deep learning-based architecture to detect attack activities in 5G-enabled UAV communications.	Achieved precise detection performance under both LoS and NLoS environments.
LLM	Decision Optimization	[23]	2023	Proposed a transformer-driven UAV trajectory planning method.	Reduced AoI and latency while mitigating the risk of data tampering.
		[21]	2024	Applied LLMs for optimizing UAV deployment and transmission power management.	Improved anti-jamming performance in emergency communication settings.
	Reasoning Enhancement	[26]	2023	Introduced an LLM-driven attack bot capable of simulating hijacking attacks on communication sessions between GCS and UAV swarms.	Improved understanding of UAV-related threats and supported stronger anti-attack strategies for UAV clusters.
		[25]	2024	Leveraged the contextual reasoning ability of LLMs to conduct semantic-level anomaly detection on blockchain-based UAV traffic data.	Enabled real-time detection of previously unseen threats without requiring retraining.
		[22]	2025	Proposed CoLLM, a distributed collaborative reasoning framework using LLMs for environments lacking a centralized ground-truth entity.	Eliminated single-point failure risks and protected against complete intelligence leakage.
	Comprehensive Analysis	[17]	2025	Conducted a comprehensive review of LLM applications in UAV security.	Emphasized the strengths of LLMs in multimodal data integration and real-time decision support.
Proposed method	LLM-Layered Collaborative Security Architecture	Ours	2025	Proposed LLM-LCSA, a cloud–edge–end hierarchical framework incorporating MoE-	Combined multi-tier LLM collaboration, adaptive expert activation, and constrained decision-

© 2023 The Author(s). | Published by Agro Intelligence Research Press

				based intelligent agents and resource-aware optimization.	making to support efficient and secure UAV swarm operations.

Table 2. Summary of existing challenges in UAV cluster security.

Problem domain	Specific challenges	Existing deficiencies
Specialized design and collaborative mechanisms	• Designing specialized security architectures tailored for UAV swarm environments • Enabling real-time state synchronization, heterogeneous data integration, and collaborative decision-making across multiple UAVs	• Current large language models are primarily designed for general-purpose natural language processing applications. • Existing approaches mainly concentrate on single-agent intelligence and lack effective multi-agent collaboration capabilities
Dynamic threat response and knowledge utilization	• Detecting sophisticated and continuously evolving threats • Dynamically incorporating expert domain knowledge into real-time decision-making processes	• Existing systems provide limited threat detection and identification performance • Insufficient support for the real-time and adaptive integration of expert knowledge
Decision optimization under resource constraints	• Enabling resource-aware intelligent decision-making in environments with constrained resources • Maintaining a balance between decision speed, accuracy, and communication resource usage	• Difficulty in achieving an effective trade-off between decision performance and multidimensional resource consumption • Limited capability to operate efficiently under restricted resource conditions

To address these obstacles, an LLM framework better aligned with UAV swarm settings is needed to detect threats and make decisions during multi-unit cooperative missions. Factoring edge collaboration use cases into the forward path for 6G networks is a significant step. This shift has already materialized across numerous domains, including vehicle-to-everything (V2X), industrial automation, and smart cities, yet concrete deployments involving UAVs remain scarce.

Hence, this work presents a security-centric, multi-unit, LLM-layered collaborative security architecture (LCSA). The design draws on a distributed data storage paradigm and resource-cognizant intelligent decision-making algorithms. Within the LLM-LCSA blueprint, the MoEs approach is housed in edge servers, a threat–expert dynamic correlation matrix is applied, and an optimization model that weighs expert recommendation costs against multidimensional resource consumption is established. Beyond that, we introduce slack variables to mediate resource conflicts, develop a multidimensional confidence scoring procedure, and embed a feedback-correction unit to enable resource-aware intelligent decision-making.

1. We advance LLM-LCSA for safeguarded multi-UAV teamwork. Through a cloud–edge–terminal cooperative computing scheme, LLM-LCSA weaves together distributed data storage, sliding-window fusion, and data validity scoring to enable multilevel model cooperative inference. In holistic performance benchmarks, every component reached top ratings.

2. An intelligent agent routine based on MoEs was formulated, implemented, and embedded in edge servers. Via the crafted threat–expert dynamic correlation matrix alongside an expert weight dynamic tuning policy, the system's accuracy in pinpointing intricate dynamic threats, together with its dynamic versatility, notably increased. Simulation tests reveal that, alongside conventional approaches, the average detection accuracy over diverse threat categories grew by 7.92%.

3. A multi-objective optimization formulation under resource constraints was developed to enable resource-aware intelligent decision-making. The formulation thoroughly accounts for expert recommendation overhead and multidimensional resource usage limits, and shapes a solution approach that introduces slack variables. Simulation outcomes show that, relative to traditional routes, the system reduces total response duration by 44.52%, thereby meaningfully improving resource efficiency.

© 2023 The Author(s). | Published by Agro Intelligence Research Press

We evaluated LLM-LCSA alongside pertinent studies, as outlined in **Table 3**. This paper makes three core contributions and addresses the current obstacles noted.

Table 3. Comparison of different methods and their features.

Methods	Ref.	Year	Dynamic adaptability	Features						
				HDF	MTD	DO	RO	RL	RM	ED
Traditional method	[32]	2022	Medium		✓	✓			✓	✓
	[33]	2023	Low	✓	✓	✓		✓		
	[34]	2023	Medium	✓	✓					✓
	[35]	2023	Low		✓				✓	✓
	[36]	2024	Low			✓	✓	✓		✓
LLM	[25]	2024	High		✓	✓				
	[22]	2025	High			✓	✓		✓	✓
	[37]	2025	High	✓		✓		✓	✓	
	[38]	2025	Low	✓	✓					✓
	[39]	2025	Medium	✓	✓	✓				
	[27]	2025	High	✓		✓			✓	✓
Proposed method	Ours	2025	High	✓	✓	✓	✓	✓	✓	✓

Note: HDF = heterogeneous data fusion; MTD = multi-threat detection; DO = decision optimization; RO = resource optimization; RL = reduce latency; RM = rating mechanism; ED = easy to deploy.

• We put forward a tiered cooperative security design that remedies the shortfalls of conventional single-layer deployment patterns when merging multisource asynchronous spatiotemporal data streams. This sharply improves data processing efficiency, with simulation evidence supporting the design's validity.

• We surmount the precision and rigidity barriers of standard hybrid expert models when facing unprecedented complex threats by introducing an online adaptive matrix. This enables on-the-fly expert triggering and continual self-refinement.

• We construct a resource-aware multi-objective optimization model to untangle the tension between decision quality and multidimensional resource drain within resource-constrained edge landscapes. By adopting slack variables and a multidimensional confidence framework, we secure the system's trustworthy behavior and rollout capacity under tight resource conditions.

The remaining sections of this paper proceed as follows: Section 2 outlines the full architecture of LLM-LCSA, a tiered cooperative security framework. Section 3 establishes the conceptual base, system formulation, and a layered cooperative threat detection algorithm. Building on the proposed system, a resource-aware intelligent decision-optimization algorithm is presented in Section 4. Section 5 unpacks the simulation findings, demonstrating the potency of the proposed architecture and algorithms. The study's conclusions and prospective research paths are laid out in Section 6.

© 2023 The Author(s). | Published by Agro Intelligence Research Press

System Architecture Design

To address the delay constraints and rigid threat-handling gaps in centralized LLM setups, this paper presents a tiered cooperative architecture, LLM-LCSA. Through the joint operation of a cloud–edge–end layered model and a built-in intelligent-agent decision apparatus, this design enables efficient multi-unit teamwork in protection-critical contexts. As shown in **Figure 2**, compact models reside on end units, mid-sized models sit on edge servers, and sizable models run in the cloud. This arrangement supports data collection, real-time processing, long-term prediction, and safety pattern evaluation.

© 2023 The Author(s). | Published by Agro Intelligence Research Press

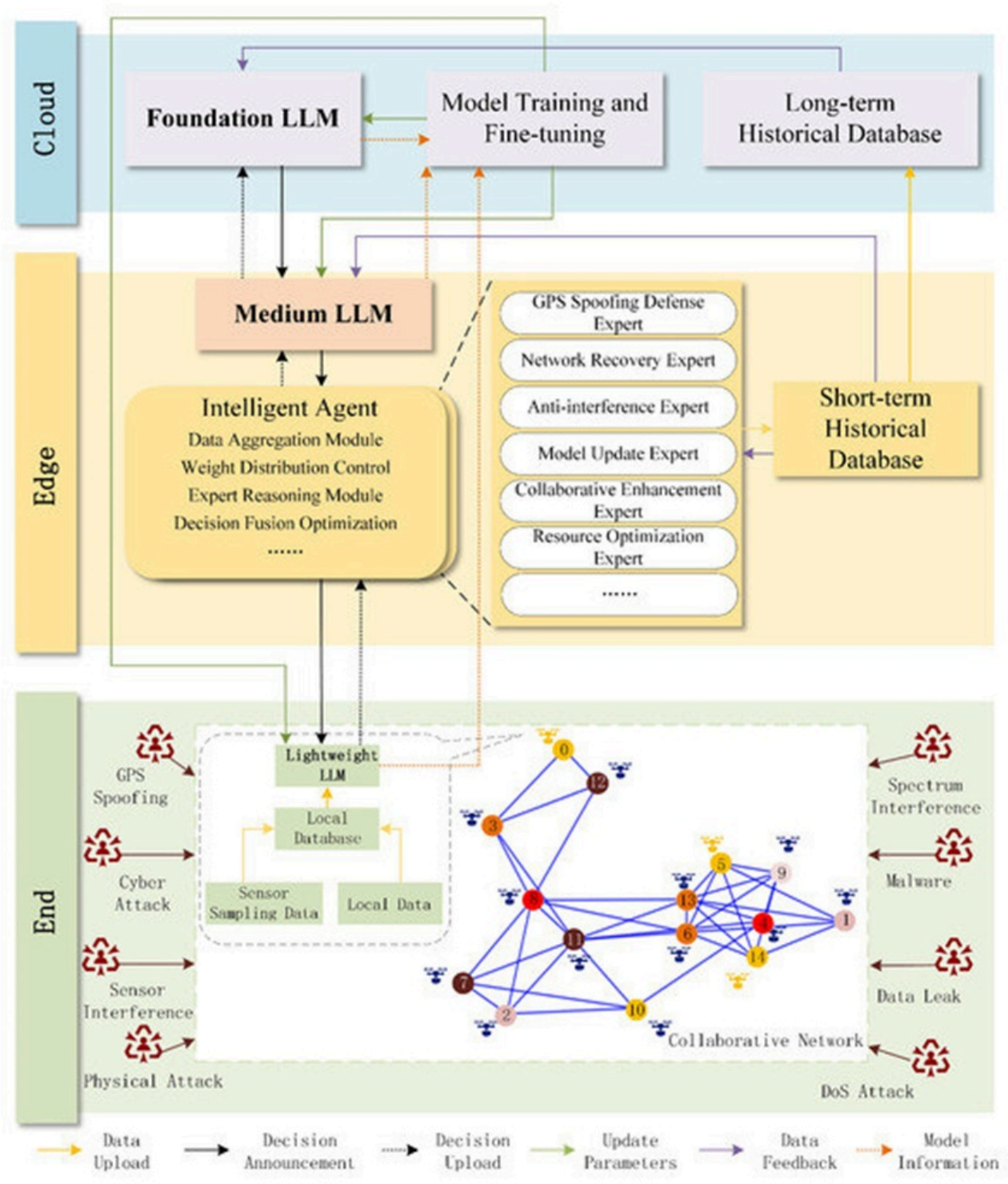


Figure 2. Architecture of LLM-LCSA.

Cooperative deployment of layered models

The bedrock of LLM-LCSA lies in the cooperative siting of tiered models to fully unlock the benefits of diverse computing pools, enabling swift data manipulation and decision support. The compact model on the end unit handles live data intake and early anomaly flagging, poised to react to variations in local sensor feeds quickly, generate anomaly detection scores

© 2023 The Author(s). | Published by Agro Intelligence Research Press

ϕ, and forward them to the edge node. The mid-sized model positioned on the edge nodes fuses anomaly detection scores from multiple UAVs with near-term historical data traits S to run sharper binary anomaly screening and derive performance indicator vectors M. The sizable model located in the cloud focuses on long-range sequence projection and expansive security pattern mining, producing long-term sequence prediction outputs T and broad security analysis outputs K. LLM-LCSA also manages offline training and tuning of the model, disseminating revised model weights to edge and end nodes.

Through this tiered model of cooperative placement, LLM-LCSA can fully capitalize on the near-instant reflexes of the end, the number-crunching heft of the edge, and the synoptic analytical scope of the cloud to refine the entire chain from data capture to decision aid. The compact model on the end side can nimbly handle local data shifts, the mid-sized model on the edge side can handle local data and render early judgments, and the sizable model in the cloud can provide a panoramic lens and deep interpretation. The three models operate in tandem to ensure streamlined coordination and intelligent decision-making for UAV swarms operating in tangled environments.

Distributed data storage architecture

To process the large, rapid, mixed data torrents generated by UAV swarms, LLM-LCSA was engineered with an original distributed data storage architecture. Short-range and long-range historical databases act as repositories for fresh data slices and overarching trend and pattern records, respectively.

The short-range history database is hosted on edge servers and stores data from the previous few minutes to several tens of minutes, capturing statistical descriptors such as anomaly rate, mean, and dispersion. These records provide instant situational context to edge medium models, enabling rapid anomaly detection and decision support. The long-range history database is housed in the cloud, retaining data for hours, days, or longer, covering cyclic tendencies and statistical summaries of prior anomaly footprints. These records equip large-scale cloud models with a global perspective, enabling long-range sequence projection and wide-angle security pattern analysis.

To better handle multisource asynchronous data, LLM-LCSA employs time-window sliding fusion and data validity scoring protocols at the edge layer. Time window sliding fusion uses an exponentially weighted moving average to give newer data greater weight, preserving data freshness. Data validity scoring measures the freshness of data from each feed through a timeliness function. When a feed becomes intermittently unavailable, historical data imputation is performed at the edge layer to fill gaps, or a degraded mode is triggered to preserve data integrity and trustworthiness. Additionally, quality yardsticks for data fusion are set for the system. Whenever those yardsticks fall below predetermined thresholds, supplementary data calls are made, or the decision confidence floor is raised to further polish the data processing pipeline.

This distributed data storage blueprint not only addresses the challenge of time-aligning and unifying asynchronous multisource data but also captures the live-data edge at the end, alleviating the bottlenecks inherent in conventional centralized data-handling modes in UAV swarm settings and establishing a robust data foundation for the secure orchestration of UAV swarms.

Embedded intelligent agent algorithm

A further linchpin of LLM-LCSA is the intelligent decision-making algorithm baked into the edge server. This agent routine rests on the MoEs paradigm; folds in task splitting, delegation, and decision merging capabilities; and weaves in domain specialist insight. The routine can shrewdly summon the most fitting expert knowledge for decision-making guided by live threat postures.

The primary modules of the agent routine encompass data fusion, weight delegation and steering, expert inference, decision synthesis, feedback and incremental tuning, and cooperative augmentation units. The data fusion unit blends data from separate tiers using methods such as timestamp synchronization and sliding-window fusion to form a

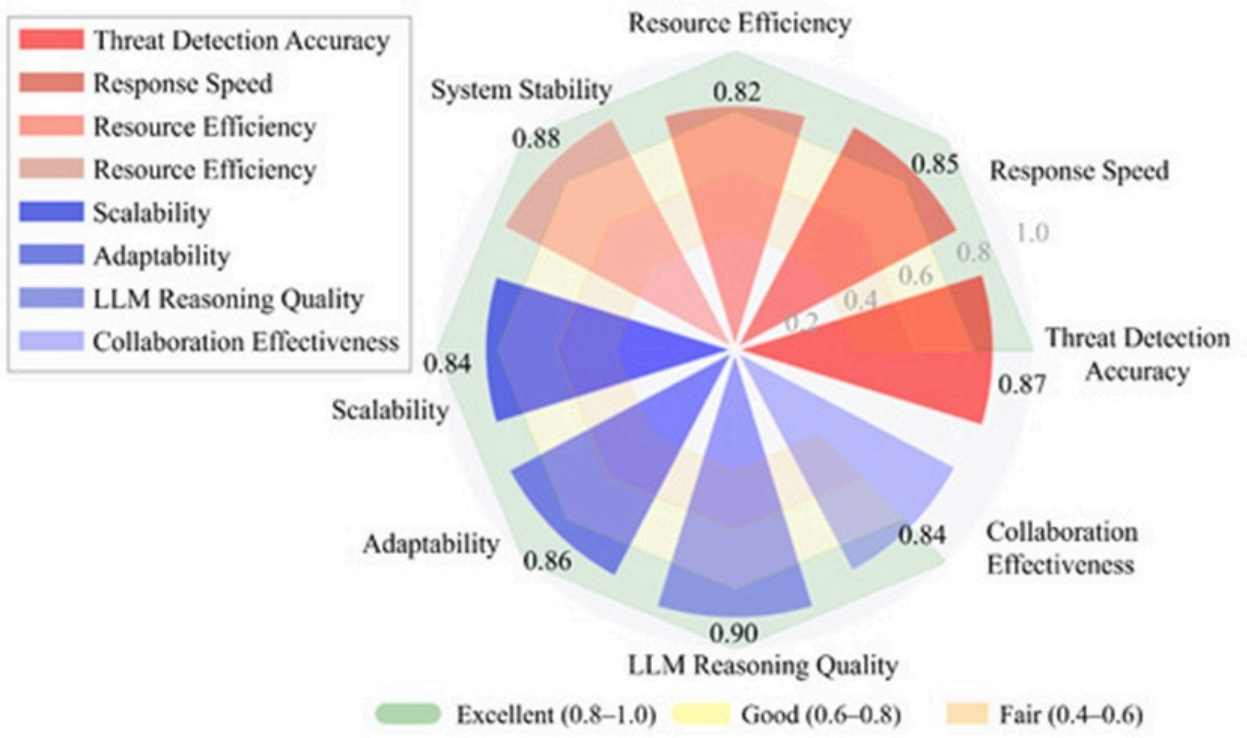
© 2023 The Author(s). | Published by Agro Intelligence Research Press

consolidated feature vector. The weight delegation and steering unit elastically modulates the influence of each expert, conditioned on the input features, to ensure that the most on-point expert judgments are accentuated across varying threat scenes. The expert inference unit allows each expert to emit a recommended decision vector grounded in their domain mastery, accommodating the live expansion and refresh of the expert pool. The decision synthesis unit polishes decision vectors by specifying cost functions and resource-drain models to ensure task needs are met while squeezing out peak resource efficiency. The feedback and incremental tuning unit employs a multidimensional confidence scoring apparatus to gauge decision quality in real time and self-corrects, informed by feedback, to sustain system resilience and pliancy. The cooperative augmentation unit also supports stratified governance and conflict arbitration for large swarms, thereby increasing the system's overall cooperative throughput.

Thanks to the embedded intelligent agent routine, LLM-LCSA not only performs efficient multi-unit orchestration and smart decision-making but also fluidly shifts decision strategies in step with live threat dynamics, markedly bolstering the system's ability to counter intricate and emerging threats and delivering potent intelligent reinforcement for the safe coordination of UAV swarms.

Performance evaluation

We measured the overall capability of LLM-LCSA using a broad set of indicators covering threat identification accuracy, response time, resource consumption, and system growth potential. The framework sets tailored assessment benchmarks matched to the primary duties of each piece. Every heterogeneous indicator is standardized, then weighted and pooled based on its relative contribution to the system's total performance. The figures are mapped to a unified score range of 0 to 1, enabling even-handed cross-module comparisons. The fine-grained experimental setup, evaluation standards, and comparative outputs appear in Section 5. As shown in **Figure 3**, all indicators exceed 0.82, indicating strong performance. LLM inference quality emerges as its most outstanding trait, with no obvious weak points, even though resource thrift could still be boosted.



© 2023 The Author(s). | Published by Agro Intelligence Research Press

Figure 3. Comprehensive performance dashboard of LLM-LCSA.

LLM-LCSA adeptly fills gaps in current UAV frameworks, including multi-platform cooperation protocols, data handling and warehousing, shifting threat countermeasures, resource-limited decision calibration, and system scalability and versatility. LLM-LCSA delivers a lean, intelligent, and growth-ready system solution for the secure, harmonized operation of UAV collectives.

System Model and Analysis

The LLM-LCSA strategy investigated in this paper is designed for a swarm of N UAVs that jointly tackle missions in complex landscapes rife with potential fluid security hazards.

System models

Network topography

The swarm employs a spread-out communication scheme. Nearby signals shuttle among UAV nodes through wireless links. Let $G=(V, E)$ denote the communication graph, with $V=\{\text{UAV1}, \text{UAV2}, \ldots, \text{UAV}N\}$ as the node assembly and E as the edge assembly, meaning that direct exchange can happen between nodes. The normalized communication span parameter appears as ($0 < dcomm \leq 1$), and an edge $(i, j) \in E$ exists between nodes only when their Euclidean separation meets $(i, j) \leq dcomm$. Edge servers are located at designated coordinates or onboard certain UAVs and handle data fusion and processing within local areas. The cloud contributes worldwide computation and warehousing support.

Threat model

The system faces M potential threat classes $Tthreat = \{T1, T2, \ldots, TM\}$. Threats can surface alone or in combination and possess a fluid, surreptitious quality. The reach of threat effects may cover a single airframe, a regional subcluster, or the whole assembly.

Data processing flow

End: Every UAV carries a lightweight LLM tasked with live gathering, preprocessing, and initial anomaly spotting of local sensor feeds, churning out preliminary anomaly scores $(t) \in \mathbb{R}$.

Edge: Medium-scale LLMs together with intelligent agents execute on edge servers. Edge servers receive (t) plus local data dispatched by UAVs inside their zone, merge them with near-term statistical descriptors $S(t) \in$ kept in a short-duration historical repository, conduct threat classification alongside local situational awareness, and generate performance metric vectors $M(t) \in$ along with provisional decision proposals.

Cloud: A large-scale LLM operates in the cloud. Pooled inputs stream in from all edge nodes together with global trend and pattern archives stored in the long-duration historical repository (t). Far-horizon projection $(t) \in \mathbb{R}^{\mathrm{m}}$ and a broad security pattern evaluation is carried out to assign security labels $K(t) \in \mathbb{N}$. Offline model coaching, fine-tuning, and parameter distribution all occur in the cloud.

Resource constraints

The setup involves eight sorts of essential resources, with the system resource availability vector given by $R=[R1, R2, \ldots, R8]^{\top}$. $R1$ through $R8$ map to computing muscle, communication bandwidth, data storage, model storage, energy draw boundaries, RAM size, link quality specifications, and sensor assets, respectively.

Inside the limits of resource accessibility, the system has to craft the best cooperative decision vector $x=[x1, x2, \ldots, xn]^{\top}$ corresponding to diverse control parameters. Putting into effect each decision element xj triggers resource draw (xj), capturing the claim on the k-th resource when decision xj is realized as follows:

© 2023 The Author(s). | Published by Agro Intelligence Research Press

$$c_k(x) = \sum_{j=1}^{n} r_{kj}(x_j), \quad k = 1, 2, \ldots, 8, \quad (1)$$

This reconciles safety, task throughput, resource efficiency, real-time responsiveness, robustness, and flexibility.

End constraints: The end resource availability vector is expressed as

$$R^{\text{end}} = \left[R_1^{\text{end}}, R_2^{\text{end}}, \ldots, R_k^{\text{end}}\right]^{\top}, \quad c_k^{\text{end}}(x) \le R_k^{\text{end}}. \quad (2)$$

Edge-side constraints: The edge server must service Nserve UAVs, subject to the following:

$$\sum_{l=1}^{N^{\text{serve}}} c_k^{\text{edge},l}(x_l) \le R_k^{\text{edge}}. \quad (3)$$

Expert system MoEs constraint:

$$\sum_{j=1}^{N_{\text{expert}}} w_j(t) \cdot c_k^{\text{expert,j}} \le R_k^{\text{edge}} \cdot \alpha_{\text{MoE}}, \quad (4)$$

Where αMoE$\in$(0, 1) stands for the slice of computational resources earmarked for the expert system.

Global resource balancing constraint:

$$\sum_{l \in \{\text{end,edge,cloud}\}} c_k^l(x) \le R_k^{\text{total}}. \quad (5)$$

Load balancing constraint:

$$\text{LI}_k = \frac{\max_l c_k(x) - \min_l c_k(x)}{\bar{c}_k(x)} \le \text{LI}_{\text{threshold}}. \quad (6)$$

Time coupling constraint: The time-bound character of resource usage is factored in as:

$$\sum_{\tau=t}^{t+\Delta T} c_k(x(\tau)) \le R_k \cdot \Delta T \cdot \phi_k, \quad (7)$$

Where $\phi k \le 1$ marks the upper bound of resource utilization.

Feature vectors and data freshness

© 2023 The Author(s). | Published by Agro Intelligence Research Press

To maintain data currency, an agent relies on the most recent records within a designated time frame when fusing streams from multiple sources. Let (t) be the fused feature vector at moment t, assembled from the following ingredients:

$$v(t) = [\phi(t), \quad M(t), \quad S(t), \quad L(t), \quad T(t), \quad K(t)]^{\top}, \quad (8)$$

Where $\phi(t)\in\mathbb{R}$ is the end anomaly detection score, $M(t)\in\mathbb{R}^4$ is the edge model performance vector, $S(t)\in$ captures short-duration historical traits, $L(t)\in$ captures long-duration historical traits, $T(t)\in$ represents cloud-based time series forecasting, and $K(t)\in\mathbb{N}$ marks safety analysis labels.

The validity score for data u at moment t is determined as:

$$f_{\text{fresh}}(u, t) = \exp\left(-\lambda \cdot \frac{t - t_u}{T_{\text{half}}}\right), \quad (9)$$

Where λ governs the decay steepness, and Thalf signifies the half-life of the data.

For short-duration time series data (t), the exponential weighted moving average prescription is used:

$$S_{\text{agg}}(t) = \sum_{k=0}^{W-1} \alpha^k \cdot S(t - k\Delta t), \quad \alpha \in (0, 1), \quad (10)$$

Where W denotes the sliding window breadth, tuned adaptively by the data sampling pace, and φ stands for the data retention ratio:

$$W(t) = \left\lceil \frac{\log(1 - \varphi)}{\log \alpha} \right\rceil. \quad (11)$$

3.3. Threat–expert association matrix

The threat type space $\mathcal{T}$={1, …, M}, the expert pool $\mathcal{E}$={1, …, Nexpert}, and the association matrix $R\in\mathbb{R}^{M\times N\text{expert}}$ obey:

$$R_{ij} = P(\text{Expert } j \text{ activated} \mid \text{Threat type } i \text{ appeared}), \quad (12)$$

Where M tallies the conceivable threat types, Nexpert tallies the experts, and Rij captures the bond strength between threat type i and expert j.

Extracting the threat features (t) yields:

$$h_{\text{threat}}(t) = \sigma(W_{\text{ext}} \cdot v(t) + b_{\text{ext}}), \quad (13)$$

Where (·) is the ReLU activation function, Wext$\in\mathbb{R}M\times$dim(v) is the weight matrix, and $b$ext is the bias term adjusting the decision frontier.

© 2023 The Author(s). | Published by Agro Intelligence Research Press

The significance weights wi for every expert are derived via the control module as:

$$w_t = \frac{\exp\left(G_t\left(v\right)\right)}{\sum_{f=1}^{N_{\text{expert}}} \exp\left(G_f\left(v\right)\right)}, \quad (14)$$

Where (v) gives the base relevance score of expert i, indicating the fit between input feature v and expert i.

On the foundation of threat-informed expert weight tuning, the threat likelihood gets multiplied by the correlation matrix to reshape the control module output:

$$\widetilde{G}_t\left(v\right) = G_t\left(v\right) + \beta \cdot \sum_{f=1}^{M} p_f^{\text{threat}} \cdot R_{ft}, \quad (15)$$

Where p_j^threat =softmax(Wth$h$threat) yields the probability of each threat type, Wth is the threat space transformation matrix, and β∈[0, 1] is the dial governing the force of threat sensitivity. At β=0, only bare gate control is in play; at β=1, the setup leans entirely on threat sensitivity. Rji marks the correlation matrix, capturing the linkage between threat type j and expert i.

The closing expert weight is computed as:

$$w_t\left(t\right) = \frac{\exp\left(\widetilde{G}_t\left(v\right)\right)}{\sum_{f=1}^{N_{\text{expert}}} \exp\left(\widetilde{G}_f\left(v\right)\right)}. \quad (16)$$

Steered by decision result feedback, the association matrix gets refreshed at intervals:

$$R_{ft}^{\text{new}} = R_{ft}^{\text{old}} + \eta \cdot f_{\text{score}} \cdot p_f^{\text{threat}} \cdot w_t. \quad (17)$$

Where η represents the learning rate, and $f$score denotes the quantitative measure of decision potency.

Expert reasoning module

The decision quantity takes the shape of a vector x=[x1, x2, …, xn] $^{\top}$, with each slot linked to a separate control lever (e.g., evacuation magnitude x1, connection handover x2, or interference suppression x3). Grounded in the input v, every expert xi puts forth a proposed decision vector di=[di1, di2, …, din]. Relying on their niche know-how, experts can contribute nonzero proposal values across one or multiple decision slots.

The aptitude rating rule for newly inducted experts is set out as:

$$C_t^{\text{expert}} = \frac{1}{|D_{\text{test}}|} \sum_{v \in D_{\text{test}}} f_{\text{score}}\left(d_t, d_{\text{reference}}, v\right), \quad (18)$$

© 2023 The Author(s). | Published by Agro Intelligence Research Press

Within which Dtest signifies the test case collection, $d$reference represents the gold-standard decision vector mirroring the system's acknowledged optimal pick under a particular input feature context, and $f$score gauges the likeness score between the expert proposal and the gold-standard decision. Upon a fresh expert's enrollment, the setup follows a guarded path to amplify the expert's clout progressively:

$$w_{l,\text{new}}^{(t)} = \min\left(\gamma \cdot w_{l,\text{new}}^{(t-1)},\ w_{l,\max}\right), \quad (19)$$

Where γ > 1 acts as the expansion multiplier and wi,max designates the upper cap on expert weight, which climbs stepwise in step with the aptitude score.

Among experts bearing overlapping remits, resource division is adaptively rebalanced against historical track records:

$$r_l = \frac{\exp\left(\lambda \cdot f_l^{\text{perf}}\right)}{\sum_{j \in \text{same group}} \exp\left(\lambda \cdot f_l^{\text{Perf}}\right)}, \quad (20)$$

Where ri stands for the share of computing assets secured by expert i, f_i^{Perf} indicates their historical performance yardstick, and λ moderates the strength of competition.

Algorithm 1 spells out a stratified cooperative threat identification procedure that pulls off three-echelon cooperative identification at the end (live), edge (consolidation), and cloud (planetary) echelons. At the end echelon, a lightweight LLM turns out anomaly scores ϕ in real time. At the edge echelon, a medium LLM consolidates short-horizon historical records and undertakes anomaly categorization. At the cloud echelon, a large-scale temporal LLM scrutinizes long-horizon patterns and allocates security labels. Time-window sliding consolidation and data-freshness fade functions maintain the data's live relevance.

© 2023 The Author(s). | Published by Agro Intelligence Research Press

- **Input:** Real-time sensor data stream from UAV clusters $\{Si(t)\}$
- **Output:** Threat probability Pthreat, threat type Ttype

Initialization:
End←Lightweight-Model
Edge←Medium-model
Cloud←Foundation_Model_T, Foundation_Model_K
SDB←Connect to short-term historical database
LDB←Connect to long-term historical database
α←0.85, λ←0.3, Thalf←10, rcloud←0.7
W←Initial time window size
for each UAVi in Cluster **do**
$\phi i(t)$←End Model .infer($Si(t)$)
Send (UAVIDi, $\phi i(t)$, timestamp) to edge servers
end for
Receive $\phi i(t)$ from all UAVs
Sagg(t)←0
Calculate Sagg(t) for $0 \le n \le W-1$ according to Equation (3)
Calculate freshness[u] for each data source u according to Equation (2)
Build $\mathbf{v}(t)$ according to Equation (1)
[Pthreat, Ttype]←Edge Model.predict($\mathbf{v}(t)$)
if Pthreat>rcloud **then**
Tpred←CloudModel_T.predict(LDB.query(last_24h))
Klabel←CloudModel_K.analyze(Tpred, $\mathbf{v}(t)$)
LDB.update(Klabel)
if Klabel==MALICIOUS **then**
Pthreat←min(1.0, Pthreat×1.2)
end if
end if
Return Pthreat, Ttype

Algorithm 1. Layered collaborative threat detection algorithm.

Complexity analysis

© 2023 The Author(s). | Published by Agro Intelligence Research Press

N denotes the tally of UAVs making up the swarm, and the complexity of end processing breaks down as: $O(N{\cdot}d)$; data reception $O(N)$; time window sliding consolidation $O(W{\cdot}d)$; data freshness calculation $O(n)$; feature vector construction $O(d)$; edge-side medium model inference $O(d^2)$; and cloud-side large-scale model manipulation $O(d^3{+}H)$ (time-series projection: $O(d^3)$, large-scale model security inspection: $O(d^3)$, and database updating: $O(\log H)$).

For $\sum_{\mathrm{i}} \mathrm{P}_{\mathrm{i}}^{\mathrm{threat}} \leq \tau_{cloud}$ with no cloud manipulation called, $\mathrm{T}(\mathrm{n},\ \mathrm{d},\ \mathrm{W}) = \mathrm{O}(\mathrm{n} \cdot \mathrm{d} + \mathrm{W} \cdot \mathrm{d} + \mathrm{d}^2 + \mathrm{n})$; for $\sum_{\mathrm{i}} \mathrm{P}_{\mathrm{i}}^{\mathrm{threat}} \leq \tau_{cloud}$ with cloud manipulation called, $\mathrm{O}(\max(\mathrm{n} \cdot \mathrm{d},\ \mathrm{W} \cdot \mathrm{d},\ \mathrm{d}^3))$

$$\mathrm{T}(\mathrm{n},\ \mathrm{d},\ \mathrm{W},\ \mathrm{H}) = \mathrm{O}(\mathrm{n} \cdot \mathrm{d} + \mathrm{W} \cdot \mathrm{d} + \mathrm{d}^2 + \mathrm{d}^3 + \mathrm{H}).$$

Intelligent Decision Optimization

The threat identification procedure described in Section 3 supplies indispensable input for the decision stages that follow. Still, fashioning ideal response tactics must account for the stringent resource ceilings native to both the UAV's end and edge computing milieus. We cast the decision optimization challenge as a bounded-cost reduction exercise and establish a closed-loop refinement cycle. Concretely, the situational awareness feature vectors (t) created by each LLM stratum operate as the shared input for downstream optimization. They not only elastically retune expert weights via the threat–expert matrix but also serve as pivotal parameters in the resource-attentive multi-objective optimization formulation to yield the optimal decision $x*$. The real-world impact of the decision is monitored in real time and translated into a feedback token. These tokens are drawn upon to renew the expert ensemble and to target the LLM's honing, thereby sculpting an unbroken loop of "sense–resolve–feedback–absorb" that fuels the system's unceasing advancement.

Resource-constrained decision optimization

The expense function of expert i is laid out as:

$$L_i(x,\ d_i) = \sum_{j=1}^{n} \alpha_{ij} \cdot (x_j - d_{ij})^2, \quad (21)$$

Inside which $\mathrm{x} = [\mathrm{x1},\ \mathrm{x2},\ \ldots,\ \mathrm{xn}]^{\top}$ is the decision vector, di quantifies the weighted divergence from its proposal, dij is the proposal value of expert i concerning decision slot j, and αij is the sensitivity weighting of expert i toward decision slot j (irrelevant slots get αij=0).

The system-wide resource availability vector is written as R=[R1, R2, …, RK], where RK signifies the ready supply of the k-th resource, and the resource bound function is composed as:

© 2023 The Author(s). | Published by Agro Intelligence Research Press

$$g_k(x) = c_k(x) - R_k \le 0, \quad k = 1, 2, \ldots, K. \quad (22)$$

The all-in expense function is put together as:

$$f(x) = f_{\text{expert}}(x) + f_{\text{resource}}(x) = \sum_{l=1}^{N} w_l \cdot L_l(x, d_l) + \lambda_r \sum_{k=1}^{K} \frac{c_k(x)}{R_k}. \quad (23)$$

Where λr is the trade-off factor for resource parsimony, modifiable on the go per the system's ongoing burden.

The resource parsimony targets are woven into optimization problems and recast as a multi-objective optimization function:

$$\min_{x \in \mathcal{X}} \left[\sum_{l=1}^{N} w_l \cdot L_l(x, d_l) + \lambda_r \sum_{k=1}^{K} \frac{c_k(x)}{R_k} \right]. \quad (24)$$

When resource limits collide, slack quantities ϵk are introduced:

$$x^* = \arg\min_{x,\epsilon} \left[f(x) + \lambda_\epsilon \sum_{k=1}^{K} \epsilon_k \right], \quad \text{s.t.} \quad c_k(x) \le R_k + \epsilon_k. \quad (25)$$

The KKT conditions deliver a closed-form expression:

$$x_j = \frac{\sum_{l=1}^{N} w_l \alpha_{lj} d_{lj} - \frac{1}{2} \sum_{k=1}^{K} \mu_k r_{kj}}{\sum_{l=1}^{N} w_l \alpha_{lj}}, \quad (26)$$

Where μk corresponds to the Lagrange multiplier, the computational footprint hinges primarily on n and K, neither of which swells notably as the UAV swarm size increases within the system, preserving the algorithm's real-time responsiveness under large-scale conditions.

Expert consensus rating

The concord metric on expert opinion appraisal reads:

$$f_{\text{consensus}} = 1 - \frac{\sum_{l=1}^{N} w_l \cdot \|d_l - x^*\|_2^2}{\max_{l,j} \|d_l - d_j\|_2^2}, \quad (27)$$

Where wi is the weight of the i-th expert, the tighter the alignment, the nearer the indicator sits to 1.

The decision results of akin historical circumstances are juxtaposed:

© 2023 The Author(s). | Published by Agro Intelligence Research Press

$$f_{\text{history}} = \sum_{(v_h, x_h, e_h) \in \mathcal{H}} f_{\text{sim}}(v, v_h) \cdot f_{\text{success}}(e_h), \quad (28)$$

Where H denotes the historical decision archive encompassing feature vectors vh, decisions xh, and results eh; $f$sim estimates the resemblance between the current feature vector and the archive; and $f$success evaluates the triumph of historical decisions.

The decision punch inside a nimble simulation testbed is rapidly corroborated:

$$f_{\text{sim}} = \frac{1}{|\text{KPI}|} \sum_{l=1}^{|\text{KPI}|} \frac{\text{Sim_KPI}_l(x^*) - \text{Worst_KPI}_l}{\text{Best_KPI}_l - \text{Worst_KPI}_l}, \quad (29)$$

Where Sim_KPI($x*$) is the ith KPI reading stemming from decision $x*$ within the testbed, and Best_KPIi along with Worst_KPIi denote the preset ceiling and floor values, respectively.

The fuzziness of the incoming data stream is appraised:

$$f_{\text{uncert}} = \exp\left(-\lambda_{\text{unc}} \cdot \sum_l \sigma_l^2\right), \quad (30)$$

Where σ_i^2 stands for the approximated spread of the ith input vector v and λunc is the scalar multiplier.

A multidimensional weighted synthesis is executed:

$$\text{Confidence}(x^*) = \sum_{m \in \{\text{consensus,history,sim,uncert}\}} \alpha_m \cdot \text{Conf}_m, \quad (31)$$

Where the αm weights can be elastically shifted via routes such as reinforcement learning to hone long-haul decision caliber.

Cutoffs are actively shifted in response to situation criticality:

$$\tau = \tau_{\text{base}} \cdot \left(1 - \beta \cdot f_{\text{Urgency}}\right), \quad (32)$$

Where τbase marks the foundational cutoff, β governs the extent to which the cutoff sinks in emergencies, and fUrgency is the live gauge of situational urgency.

When the setup involves a large number of UAVs, a cooperative augmentation element is engaged to enable sharper decision-making and operationalization. UAVs are sectioned into multiple clusters $\mathcal{G}$={$G1$, $G2$, …, Gk}, with edge servers and agents positioned within each cluster Gi=UAVi,1, UAVi,2, …}. The clusters relay condensed packets through a top-tier orchestration routine:

© 2023 The Author(s). | Published by Agro Intelligence Research Press

$$I_i^{\text{share}} = F_{\text{abstract}}\left(v_i,\ x_i^*,\ f_{\text{uncert}}\right), \quad (33)$$

Where $I_{\text{i}}^{\text{share}}$ captures a digest of information circulated by cluster i, covering critical status, decision inclination, and uncertainty estimate. Whenever a friction surfaces between neighboring cluster decisions, a bargaining procedure is set in motion:

$$f_{\text{conflict}}\left(x_i^*,\ x_j^*\right) > \theta_{\text{conflict}} \Rightarrow \text{Negotiate}\left(\text{Agent}_i,\ \text{Agent}_j\right), \quad (34)$$

The agent transmits the terminal optimal decision vector $x*$ to each concerned UAV, which subsequently executes the corresponding action (evacuation, comms swap, interference suppression, etc.) in accordance with $x*$ and reports the operational outcomes back to the system.

Multi-expert collaborative safety decision-making algorithm

Algorithm 2 details the multi-expert cooperative adaptive security decision-making workflow. The workflow extracts threat signatures, derives threat likelihood distributions, and then adaptively recalibrates expert weights informed by threat probabilities and resource matrices. Following this, it refines and produces the optimal decision vector under resource boundaries and fuses four facets—consensus strength, historical alignment, simulation validation, and uncertainty—into a holistic confidence appraisal. The workflow elastically modifies the execution threshold in response to resource scarcity to enable adaptive decision rollout.

© 2023 The Author(s). | Published by Agro Intelligence Research Press

- **Input:** $\mathbf{v}(t)$, $\phi(t)$, **R**available, Expert $\mathscr{E}$ and αji, Threat–Expert Association Matrix **R**, Historical Decision Database $\mathscr{H}$, Lightweight Decision Simulator $\mathcal{S}$
- **Ouput:** $\mathbf{x}*$, $Conf$

Initialization:

hthreat←ReLU(**W**ext·**v**(t)+**b**ext)

pthreat←(**W**th·**h**threat)

Calculate $\bar{G}j$ for $0 \leq j \leq N$ according to Equation (8)

Calculate wj for $0 \leq j \leq N$ according to Equation (9)

for j=1**to** N **do**

dj←Expert$j$(**v**(t))

end for

Calculate $\mathbf{x}*$ according to Equation (20)

Calculate $Conf$cons, $Conf$hist, $Conf$sim, $Conf$uncert according to Equations (21) and (24)

$Conf \leftarrow \sum_{m \in \Omega} \alpha m \cdot Conf m$ // Ω={cons, hist, sim, uncert},α=[0.4, 0.3, 0.2, 0.1]

$Urgency \leftarrow 1 - \min(1, \frac{\|Rused\|}{\|Rmax\|})$

τadaptive←τbase·(1−βurg·$Urgency$)

if $Conf$<τadaptive**then**

TriggerHumanIntervention($\mathbf{x}*$, $Conf$)

else

ExecuteDecision($\mathbf{x}*$)

feedback←$MonitorExecution()$

R←**R**+η·feedback·**p**threat·**w**

end if

Return $\mathbf{x}*$, $Conf$

Algorithm 2. Dynamic expert decision algorithm.

Complexity and Deployment Analysis

K denotes the number of resource classes, H the count of stored historical decision entries, n the dimensionality of the decision vector, and d the dimensionality of the input feature vector. The complexity of threat signature matrix multiplication stands at ($M \cdot d$); threat-sensitivity weight correction runs at (Nexpert·M); expert decision generation runs at (Nexpert·d); resource-bound decision optimization runs at (Nexpert·n^2+$K \cdot n$); and multidimensional confidence appraisal runs at (N^2expert·n)+O($H \cdot d$). The total complexity therefore amounts to Nexpert, M, n, d, K, H)=O($M \cdot d$+Nexpert·M+Nexpert·d+Nexpert·n^2+$K \cdot n$+N^2expert·n+$H \cdot d$). Since the expert pool size and decision dimensionality are each far smaller than the store of historical entries, this expression simplifies to T=($M \cdot d$).

© 2023 The Author(s). | Published by Agro Intelligence Research Press

Accordingly, the algorithm's complexity hinges predominantly on the volume of stored historical records, a factor that can be dialed to suit practical circumstances.

Further reflection must address obstacles that arise during field deployment, including the system's inherent robustness and transmission lag, the hardware constraints of the UAV airframe, and data confidentiality. Such elements can affect the system's real-time responsiveness and trustworthiness. To counter these obstacles and uphold system security in genuine operational theaters, LLM-LCSA handles terminal data using sliding-window merging and data freshness scoring. Feature vectors encapsulate purely statistical summaries in place of raw feeds, thereby reducing exposure of confidential information. The resource-cognizant decision engine supports counter-jamming measures such as agile channel switching and spread-spectrum techniques. Via live threat spotting enabled by end–edge–cloud cooperation, along with the on-the-fly invocation of expert models via the MoEs mechanism, ideal response choices are quickly formulated and enacted. In addition, slack quantities introduced into the multi-objective optimization model effectively mitigate security weaknesses that might otherwise arise from resource contention. The feedback assembly, grounded in multidimensional confidence appraisal, continually hones decision-making policies, collectively ensuring the system's security and privacy safeguards in complex operational settings.

To evaluate practical rollout readiness, we sized the computational resources required for agents at each tier: lightweight LLMs can be hosted on embedded hardware such as the NVIDIA Jetson Orin. In contrast, mid-sized LLMs and hybrid expert ensembles at the edge can leverage edge computing units such as the NVIDIA A100. In contrast, foundation cloud LLMs can rest on standard AI server farms. Assessment indicates that, with the current 5G/6G infrastructure and commercially available hardware, the LLM-LCSA design demonstrates considerable engineering viability, laying the groundwork for subsequent fielding and use in real UAV swarms.

Simulation and Results

The simulation experiments were carried out using PyCharm 2022.1, with the algorithms coded in Python 3.8.5. The routines were executed on a server running Windows 11 with 8.00 GB of RAM and a 13th Gen Intel(R) Core(TM) i9-13900H processor (Intel Corporation; Santa Clara, California, USA) running at 2.60 GHz. The platform supports the identification of eight threat categories (GPS spoofing, network intrusion, sensor jamming, physical sabotage, spectrum jamming, malware, data exfiltration, and DoS attack) in addition to the nominal state. **Table 4** presents the LLM-LCSA parameter settings. **Table 5** presents the experimental parameter settings.

Table 4. LLM-LCSA parameter configuration.

Category	Name	Value
Lightweight LLM	Model size	7 B parameters
	Architecture type	Lightweight inference architecture based on the Transformer model
	Inference latency	Below 15 ms
	Memory usage	Less than 2 GB
	Attention weight	GPS weighting: 0.25; communication weighting: 0.20
	Sensor weight	0.15
	Latency weight	0.10
	Spectrum weight	0.15

© 2023 The Author(s). | Published by Agro Intelligence Research Press

	CPU weight	0.10
	Memory weight	0.05
	Detection threshold	0.4
Medium LLM	Model size	13 B parameters
	Number of Transformer layers	24 layers
	Inference latency	Below 45 ms
	Memory usage	Less than 8 GB
	Input dimensions	12-dimensional feature representations
	Output dimensions	9 output classes (8 threat categories + normal state)
	Number of self-attention heads	16 attention heads
	Feedforward network dimensions	4096
Large LLM	Model size	70 B parameters
	Transformer layers	80 Transformer layers
	Inference latency	Below 180 ms
	Memory usage	Less than 40 GB
	Sequential prediction window	240 historical data points
	Context length	2048 tokens
	Pattern memory capacity	Storage capacity for 2000 threat patterns

Table 5. Simulation parameter configuration.

Category	Name	Value
UAV cluster	Number of UAVs	15 UAVs
	Flight altitude	80∼150 m altitude range
	Cruising speed	6∼10 m/s
	Maximum speed	Up to 12 m/s
	Flight area	3 km × 3 km operational area
Communication system	Communication frequency	2.4 GHz/5.8 GHz dual-band operation
	Transmit power	100 mW
	Antenna gain	2.15 dBi
	Communication range	500–1000 m
	Data transmission rate	1–10 Mbps
	Path loss index	2.2

© 2023 The Author(s). | Published by Agro Intelligence Research Press

	Shadowing attenuation standard deviation	3 dB
Network topology	Topology type	Random geometric graph structure
	Normalized connection distance	0.35
	Average node degree	4–6 connections per node
	Network diameter	≤ 5 hops
	Connectivity probability	> 95%

A performance dissection of the LLM-LCSA constituents, spanning the end LLM, edge LLM, cloud LLM, expert ensemble, resource optimization pipeline, and decision fusion pipeline, is given in **Figure 4**. The performance ratings of each LLM constituent appear in **Figure 4a**, and the response durations of each constituent appear in **Figure 4b**. The cloud-based large LLM receives the highest rating, 0.89; however, this constituent incurs the greatest delay, 195 units. The end lightweight LLM exhibits the shortest delay, curtailing reliance on the cloud and preserving system real-time properties. The three-tier architecture achieves an equilibrium between peak capability and real-time agility.

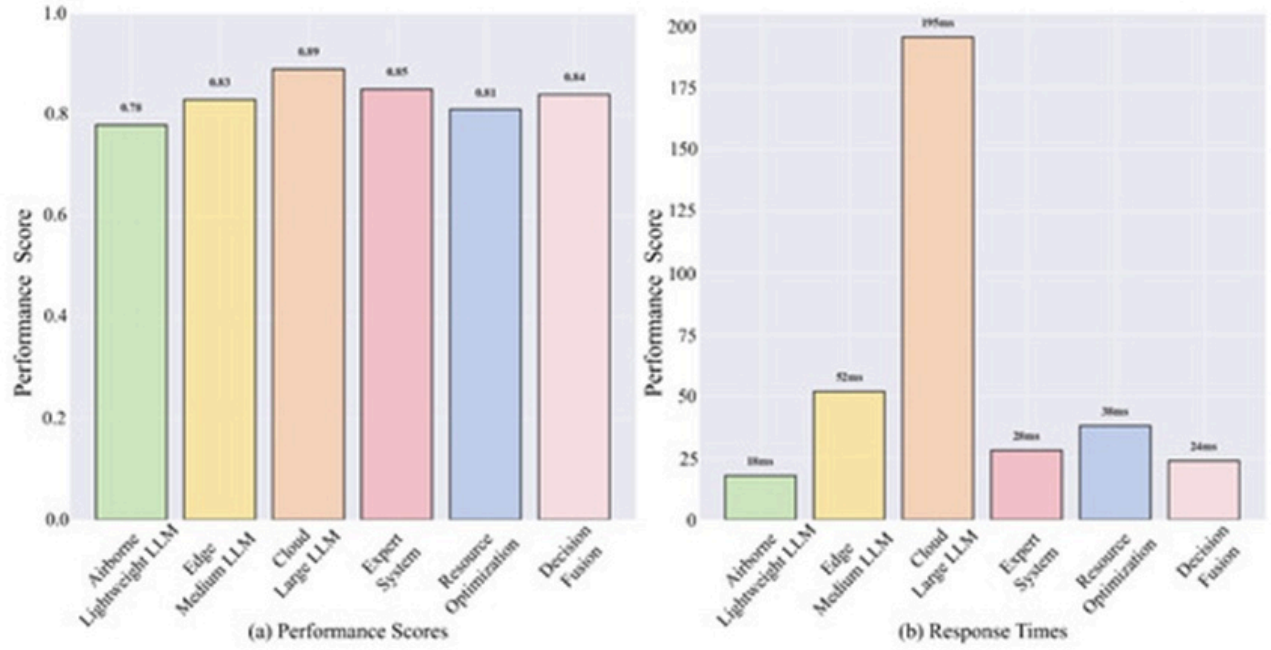


Figure 4. Component performance analysis of LLM-LCSA.

The variation in expert weights amplified by the LLM is depicted in **Figure 5**. The dynamic progression, wherein expert weights are elastically shifted in accordance with threat categories, is shown in **Figure 5a**. All expert weights oscillate within the 0-0.5 range, indicating that the system employs a balanced scheme that prevents any single expert from monopolizing the decision stream. During the initial learning window, weight distribution stays comparatively uniform. In the middle window, differentiation begins: the GPS defense expert's weight climbs markedly under GPS assault conditions, and the overarching coordination expert's weight rises amid composite threats. This intelligent cooperation scheme enables real-time weight retuning per threat category, along with knowledge exchange and renewal across the expert pool. A statistical breakdown of the weights is shown in **Figure 5b**, with an average near 0.125, consistent with the anticipated even split across the eight experts. The modest oscillations suggest the system can effect subtle calibrations shaped by threat conditions; the standard deviation envelope of roughly ±0.05∼0.08 reveals that expert weight dispersion rests at a moderate level, enabling differentiation (to address diverse threats) while avoiding excessive scatter; the peak weight crest touches approximately 0.45∼0.5, surfacing at T = 4∼5 min, matching major threat episodes, suggesting the

© 2023 The Author(s). | Published by Agro Intelligence Research Press

system can marshal decision weights at critical instants. The trough weight remains in the 0.02-0.05 range, ensuring that even the lowest-priority experts retain foundational influence, reflecting a fault-tolerant design philosophy.

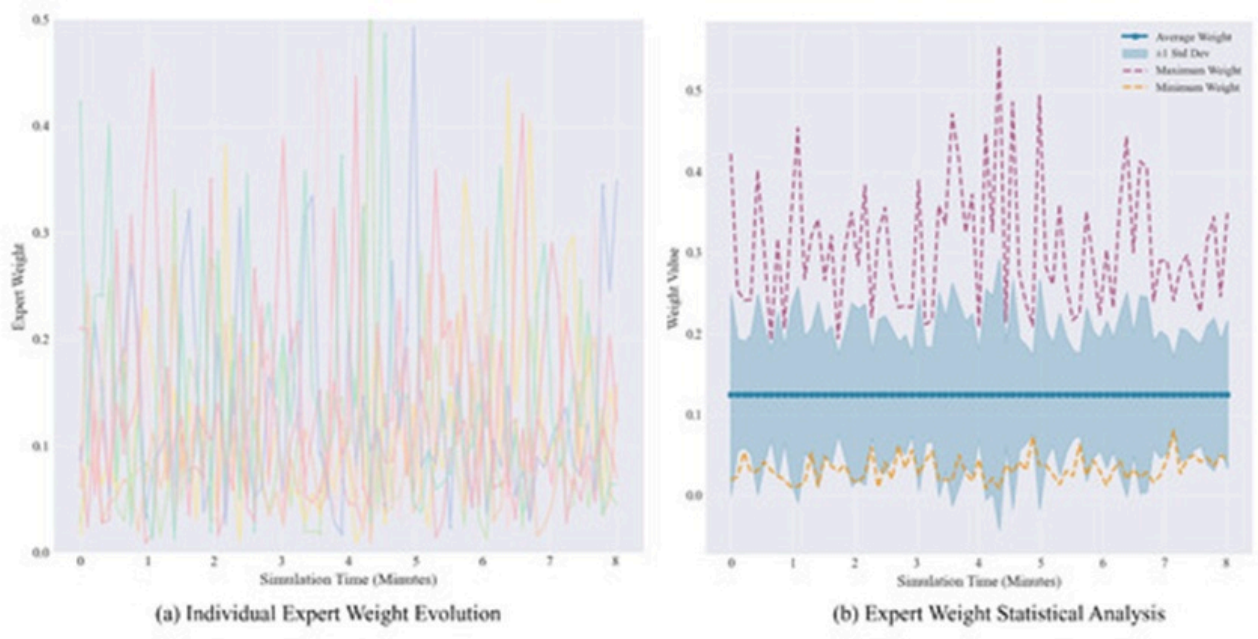


Figure 5. Changes in expert weights.

The spread of threats within a UAV network and the counteraction orchestrated by the LLMs are illustrated in **Figure 6**. A distance-based geometric representation was constructed atop 15 UAVs. For principal spread pathways, merely 1∼2 hops are required from the high-altitude node to the adjacent subgroup, 3∼4 hops for cross-subgroup links, and 4∼5 hops for the network periphery node. The LLM operates as an orchestration nexus at nodes 0, 5, 10, and 14, shouldering threat information fusion and response orchestration, executing a shielding strategy that features early intervention under mild-threat states, communication quarantine of severe-threat nodes, and joint shielding of neighboring nodes.

© 2023 The Author(s). | Published by Agro Intelligence Research Press

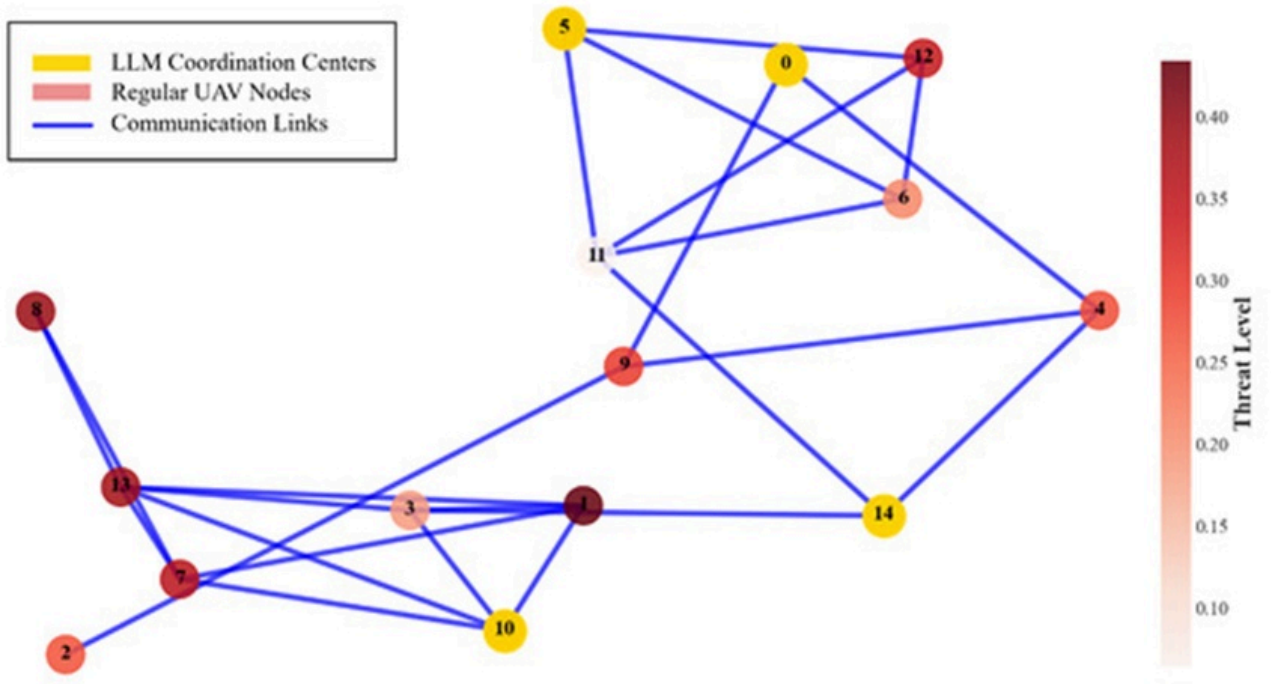


Figure 6. UAV network threat propagation and LLM-coordinated response.

Figure 7 offers a comparative view of the learning velocity and effectiveness of multiple algorithms. The LLM-LCSA trajectory exhibits the steepest ascent, denoting rapid accommodation to novel threat patterns. Conventional approaches gain proficiency more gradually and encounter learning ceilings later. Given the heterogeneous nature of threats, a single algorithm cannot reliably pinpoint them. LLM-LCSA incorporates a hybrid expert system in which several LLM components work in concert to enhance decision-making and recognition capabilities across diverse threats.

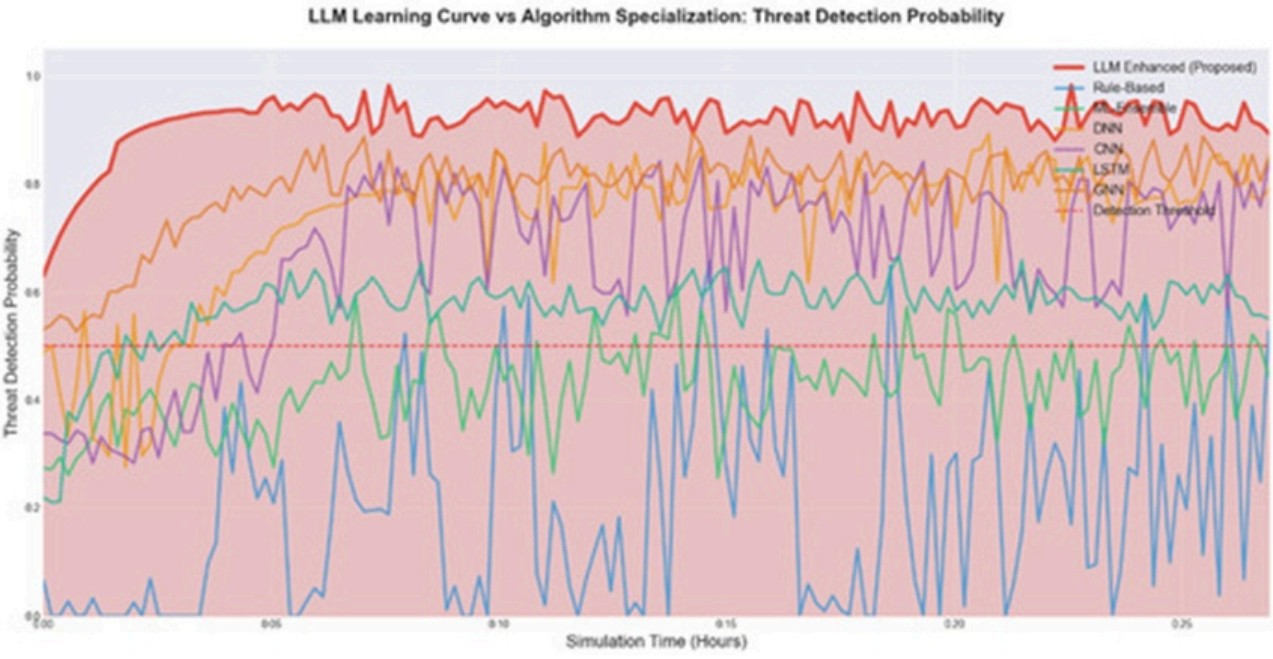


Figure 7. Learning curve and performance comparison.

© 2023 The Author(s). | Published by Agro Intelligence Research Press

As shown in **Figure 8**, LLM-LCSA consistently outperforms all baseline competitors, underscoring its resilience and broad applicability. The architecture demonstrates strong performance in detecting intricate threats, achieving 15.2% gains over GNN baselines in malware identification and 18.7% gains against GPT spoofing. This is credited to its potent fusion of multisource feeds and expert insight. Furthermore, LLM-LCSA achieves an average margin of 5.4% in flagging simpler threats, such as sensor and spectrum jamming, domains typically handled by CNN-centric approaches. Across varied attack scenarios, LLM-LCSA outperforms the leading algorithm in the comparison ensemble by an average of 7.92%, substantiating the efficacy of our hierarchical cooperative design.

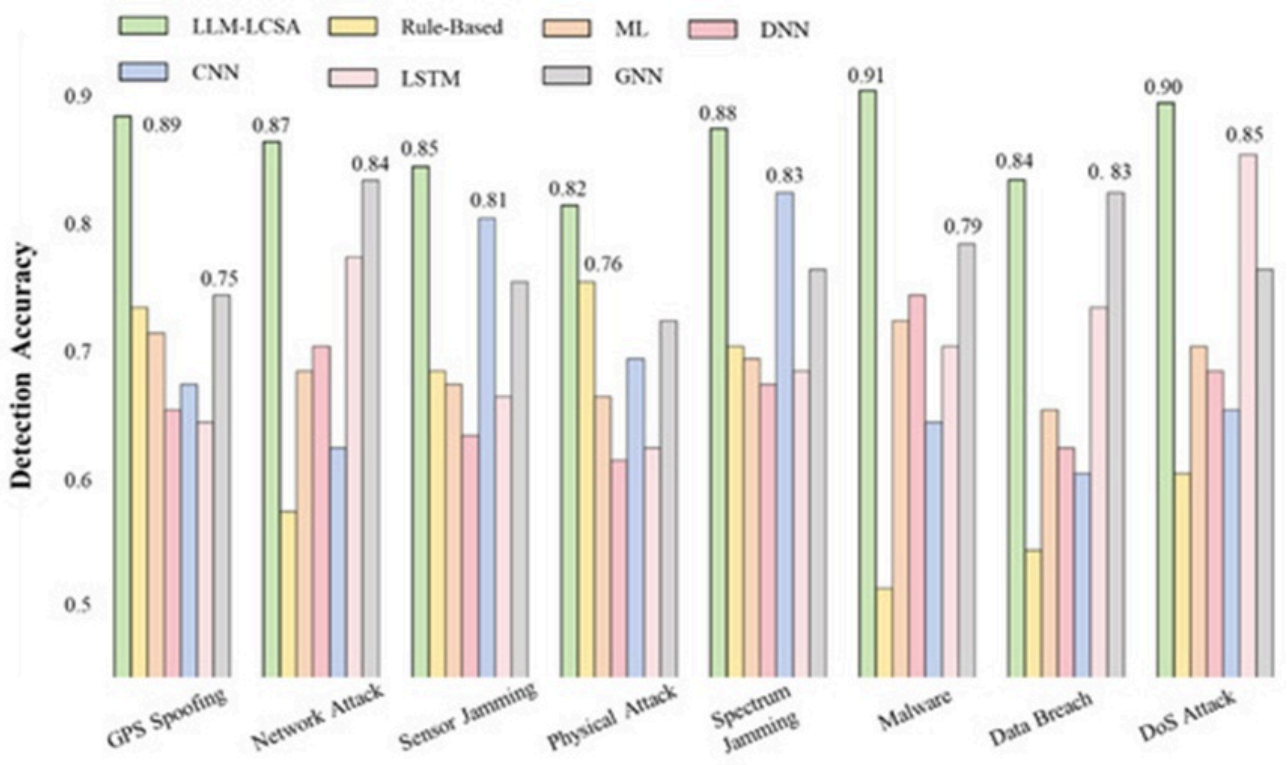


Figure 8. Threat type detection accuracy.

The consumption of eight vital resources (computational capacity, communication bandwidth, data and model storage, energy budget, RAM footprint, connection quality and delay, dedicated processing units, and sensor assets) is portrayed in **Figure 9**. Because the model requires data refreshes and interaction with external systems, its reliance on communication assets exceeds that on other vital resources. Nonetheless, this surge occurs solely around the 1.7 min mark, enabling staggered orchestration with other vital resources. At this point, no other resource experiences peak consumption, thereby realizing load distribution and averting single-point resource bottlenecks.

© 2023 The Author(s). | Published by Agro Intelligence Research Press

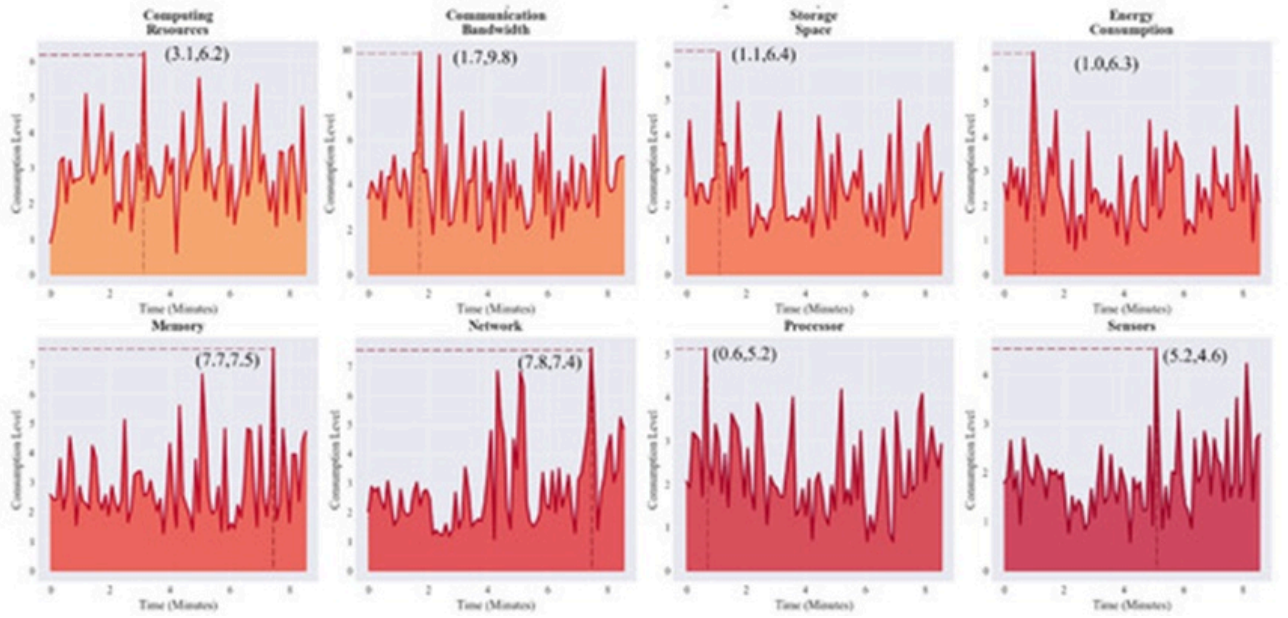


Figure 9. Resource consumption analysis.

To foreground the superiority of this architecture in cooperative response at the system tier, we additionally performed weighted blending on alternative techniques, selecting enterprise rule-based frameworks, widely adopted academic ML stacks, and distributed systems, assigning them weights of 0.4, 0.35, and 0.25, respectively, to generate a cooperative architecture emblematic of conventional approaches.

The response delay comparison is presented in **Figure 10**. The five critical response phases are: from threat emergence to detection confirmation; from detection to decision output; resource allocation and execution interval; multinode cooperative response interval; and from attack to system restoration. Measured against conventional approaches, LLM-LCSA achieves a threat detection delay of 18 ms vs. 35 ms (a 49% reduction), a decision formulation interval of 52 ms vs. 85 ms, a resource orchestration speed of 68 ms vs. 120 ms, a cooperative response interval of 95 ms vs. 180 ms, a 47% efficiency boost, a 46% cut in system restoration interval, and a 44.52% reduction in total interval. Consequently, LLM-LCSA realizes multilayer parallel computation, facilitates trend-driven proactive readiness, and compresses the response interval.

© 2023 The Author(s). | Published by Agro Intelligence Research Press

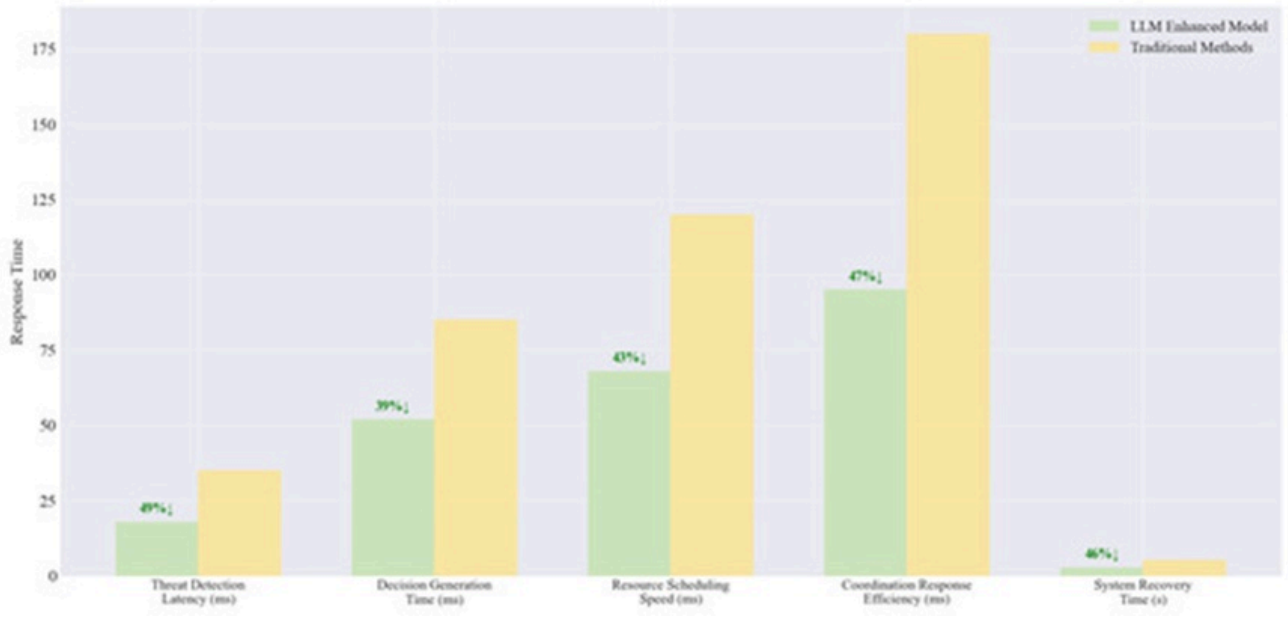


Figure 10. Response latency comparison.

The evaluation outcomes for scalability and adaptability are presented in **Figure 11**. The behavior of conventional approaches is juxtaposed with that of our framework as the UAV count rises. The performance curve of LLM-LCSA tapers off gradually, whereas that of conventional approaches falls off sharply. Once the UAV count reaches 30, the performance gap widens markedly. Across distinct adaptation contexts, LLM-LCSA secures superior ratings. Owing to its knack for perpetually internalizing fresh threat signatures, it achieves better outcomes during strategy renewal episodes.

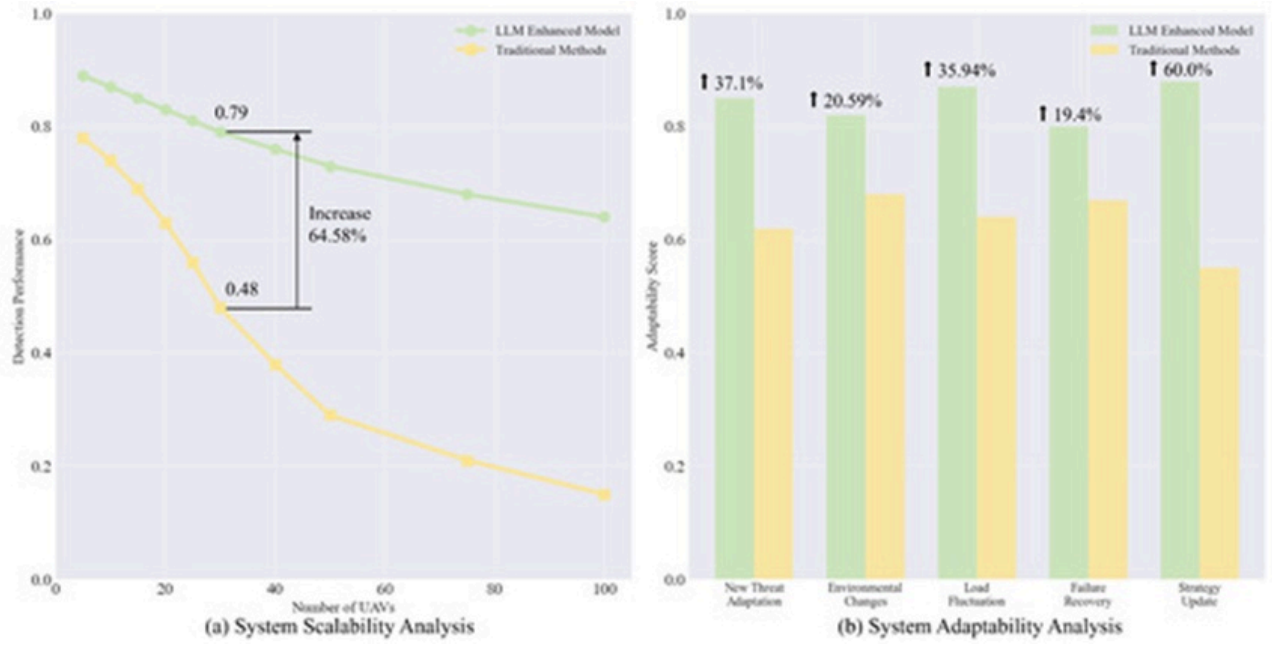


Figure 11. Scalability and adaptability analysis.

The results of the threat response timing assessment are displayed in **Figure 12**. The experiment encompassed 120 time increments, spanning roughly 13 min, each approximately 6.5 s. The examination indicates that the threat surfaced at 130 s, and by 143 s, LLM-LCSA had initiated its upgraded countermove, with the countermove's peak magnitude reaching

© 2023 The Author(s). | Published by Agro Intelligence Research Press

105.5% of the threat's peak magnitude. The countermove extended across the full duration from threat onset to dissipation, closely tracking the threat's evolution contour. Conventional approaches did not begin reacting until 97.5 time increments after threat surfacing (about 1.4 min behind LLM-LCSA), resulting in delays and insufficient countermove magnitude. Accordingly, LLM-LCSA is endowed with threat early-warning capacity, delivers more precise countermeasure magnitude, and can fully satisfy threat management requirements throughout the lifecycle.

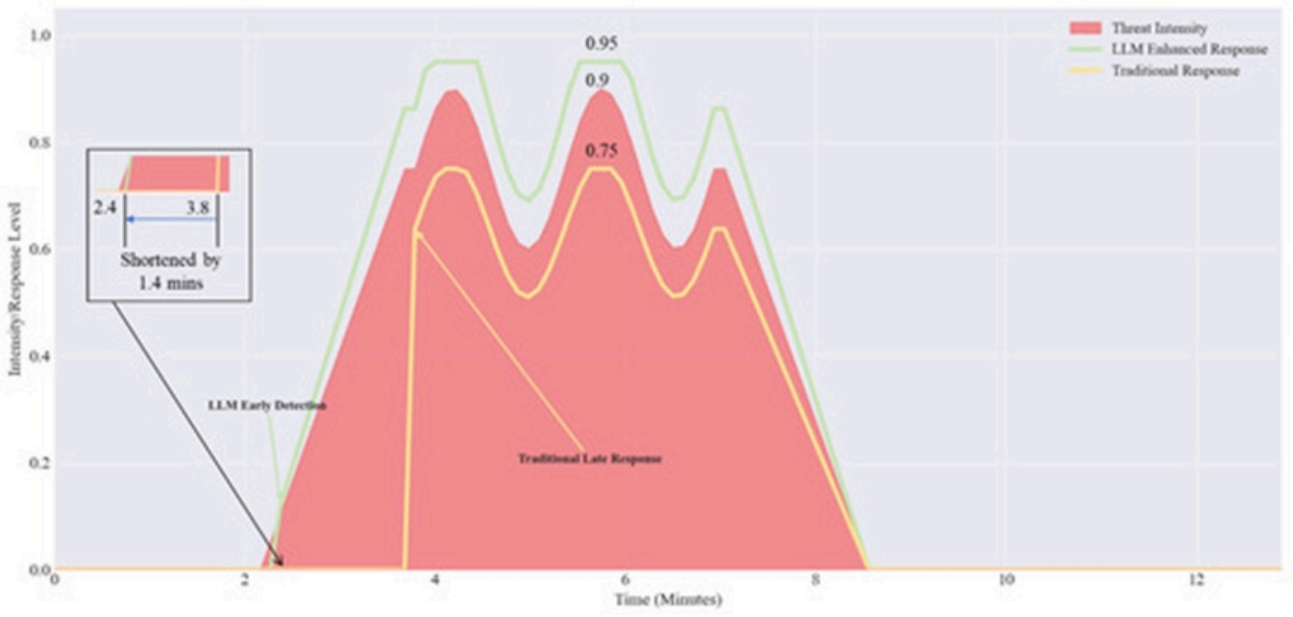


Figure 12. Threat response time series analysis.

To thoroughly evaluate the dependability of LLM-LCSA, we additionally examined its false alarm rate and miss rate. The false alarm rate captures the frequency with which the system incorrectly labels benign activity as a threat, whereas the miss rate captures the fraction of genuine threats the system neglects to flag. As illustrated in **Figure 13**, the LLM-LCSA framework recorded substantially lower false alarm and miss rates than conventional approaches across all eight threat categories. Concretely, LLM-LCSA attains a mean false alarm rate of 3.2% and a mean miss rate of 2.1%. Placed alongside conventional approaches (false alarm rate: 8.7%, miss rate: 6.5%), these numbers translate into relative declines of 63.2% and 67.7%, respectively. This result thus amply attests to the equilibrium LLM-LCSA strikes between precision and recall in threat identification.

© 2023 The Author(s). | Published by Agro Intelligence Research Press

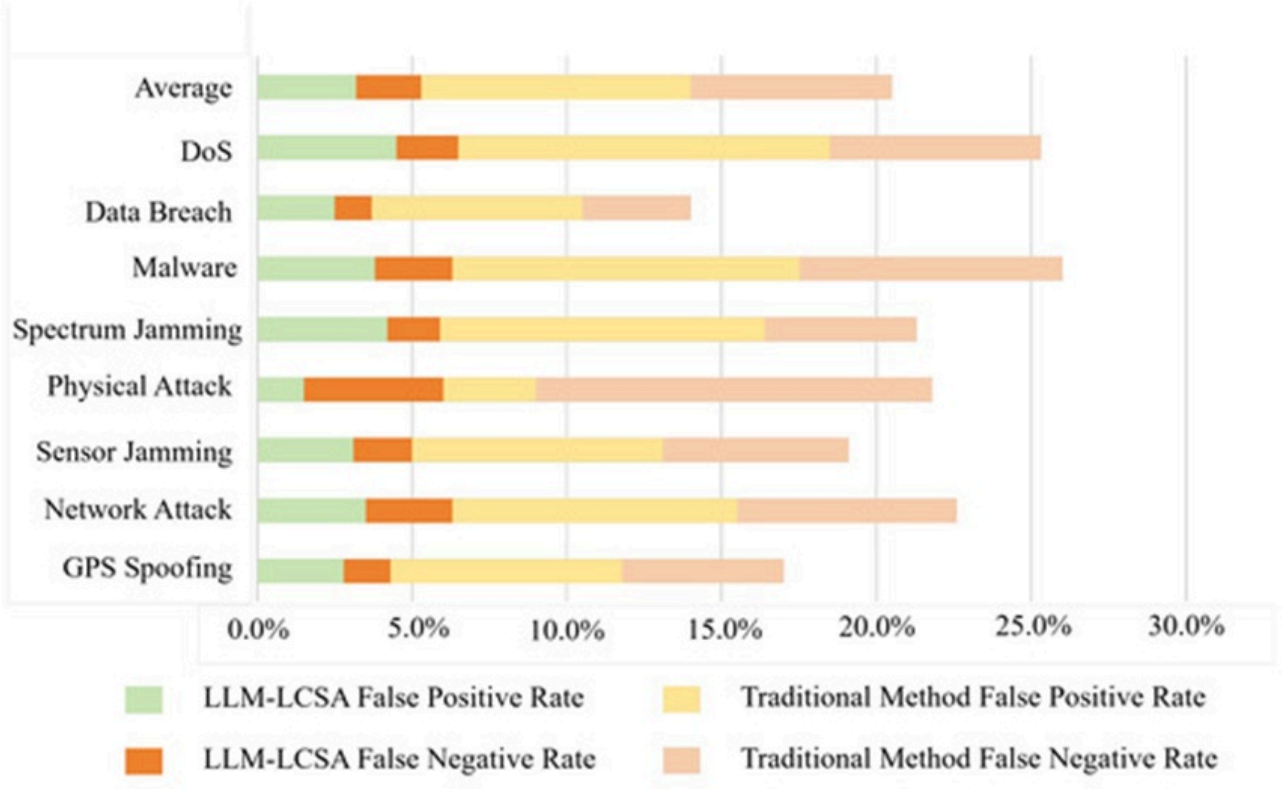


Figure 13. False positive rate and false negative rate analysis.

To corroborate LLM-LCSA's scalability, we incrementally increased the UAV count to 30, 45, and 60. **Figure 14** illustrates the response durations of each constituent. As the UAV scale broadens, the response time of cloud-based models grows most rapidly, yet it remains within a tolerable performance band. The lightweight LLM module, expert system module, and decision fusion module stayed nearly unaffected, registering response duration growth of under 2 ms. This confirms that, even as the UAV fleet swells, the system maintains real-time responsiveness with minimal additional latency.

© 2023 The Author(s). | Published by Agro Intelligence Research Press

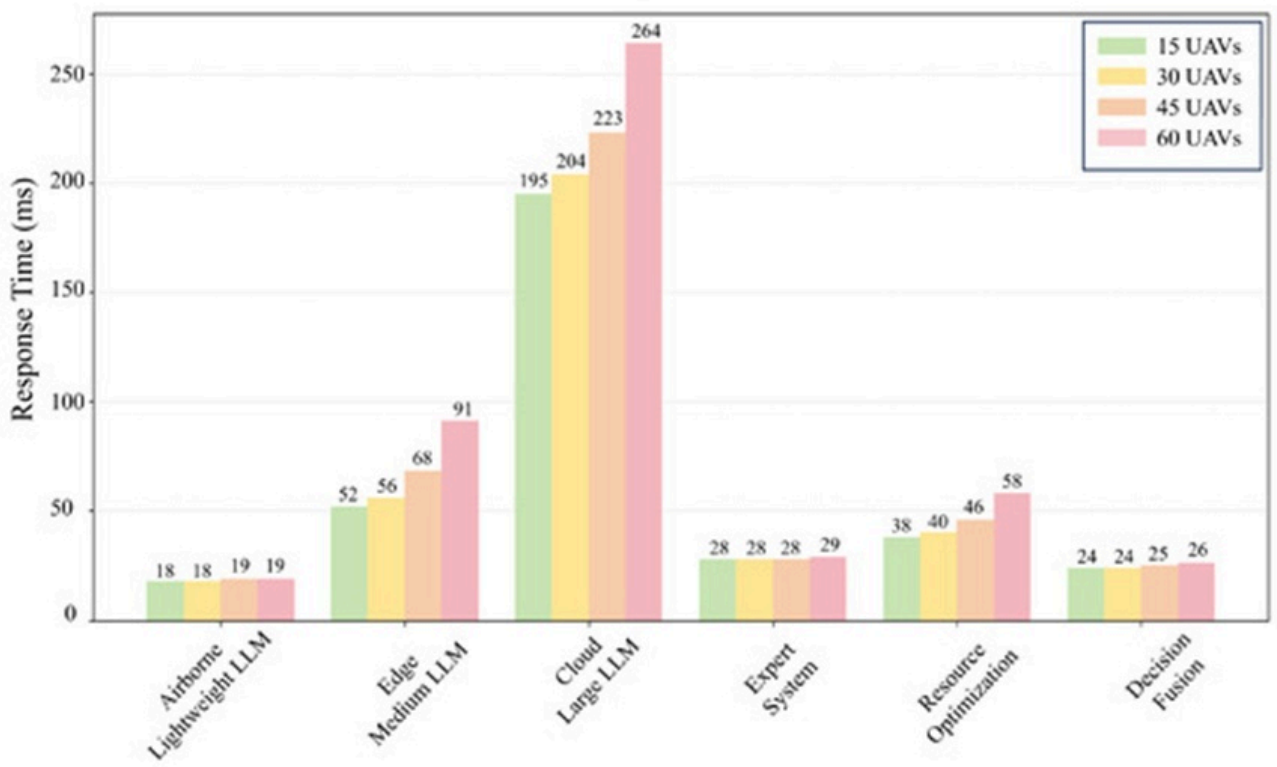
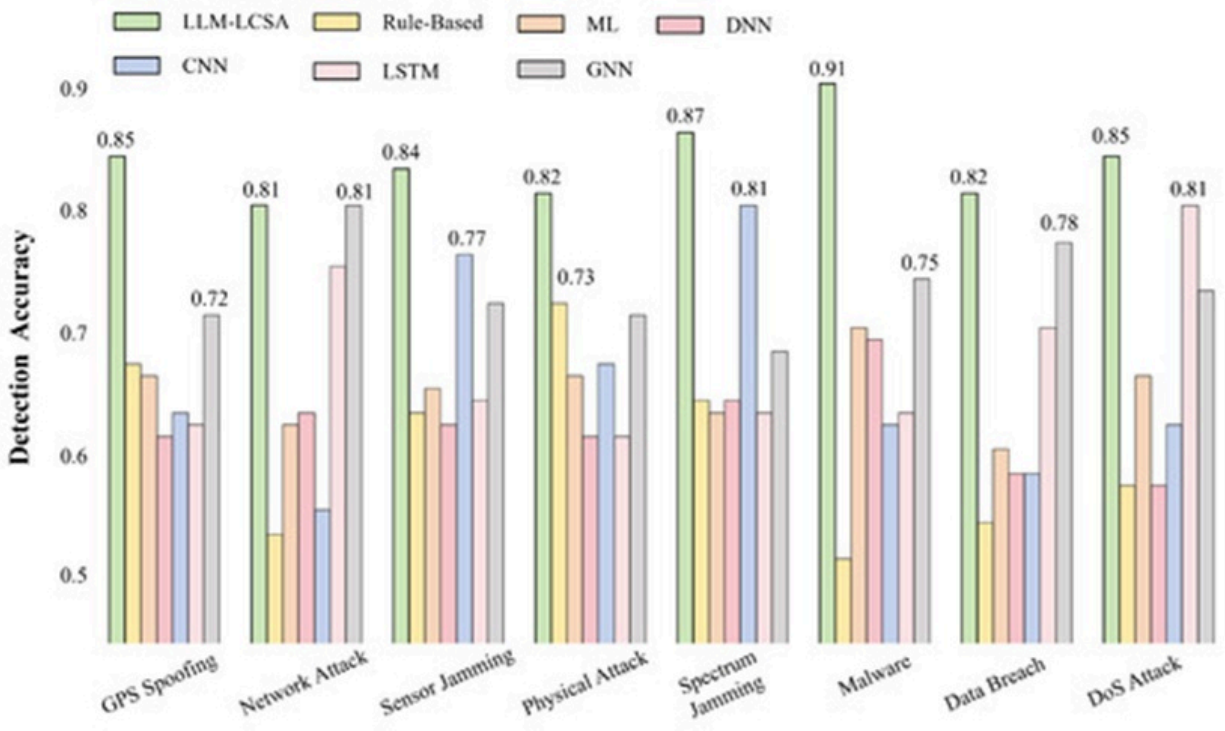


Figure 14. System response times at different UAV scales.

Figure 15 depicts the accuracy of varied algorithms against different threats when the UAV tally reaches 60. One can observe that as the UAV scale increases, the LLM-LCSA's threat identification accuracy remains relatively unchanged. In contrast, the baseline technique shows a discernible deterioration in performance.

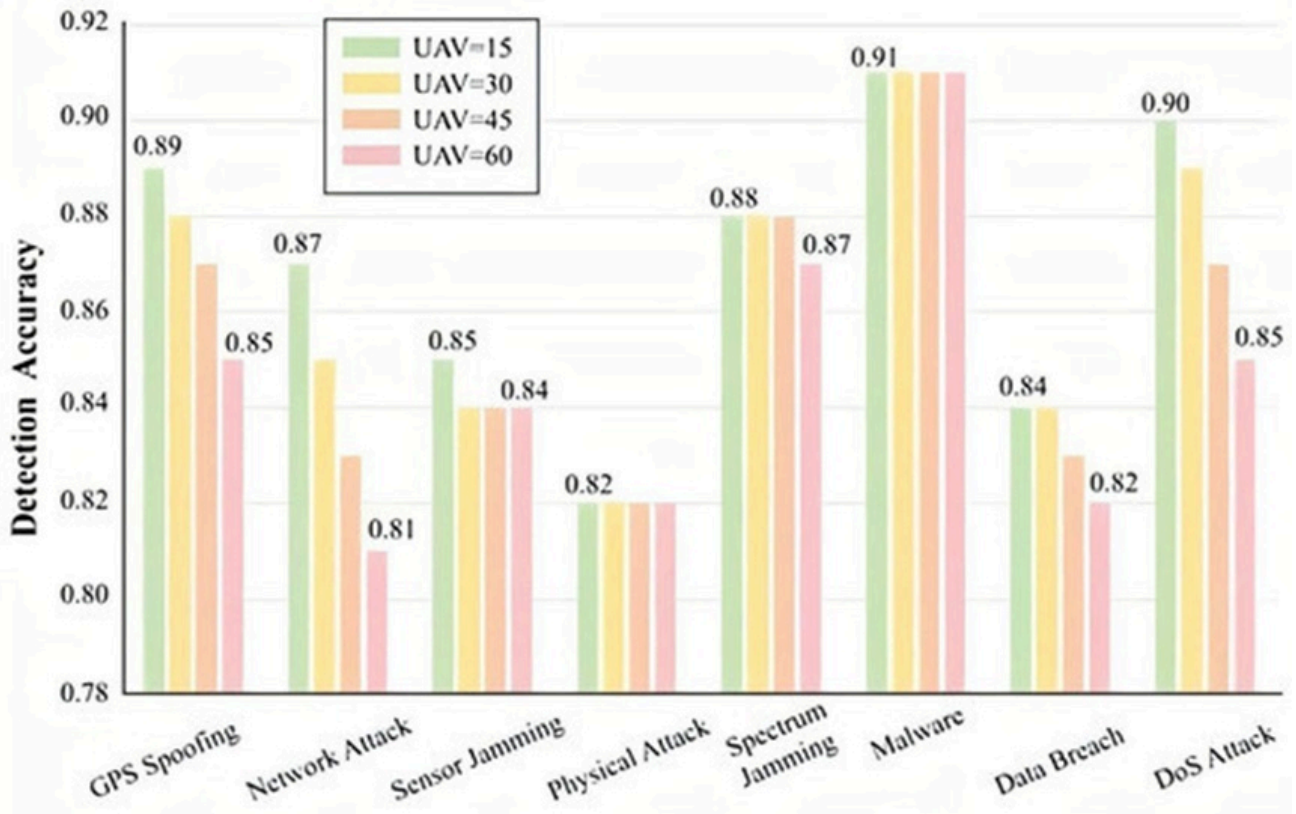


© 2023 The Author(s). | Published by Agro Intelligence Research Press

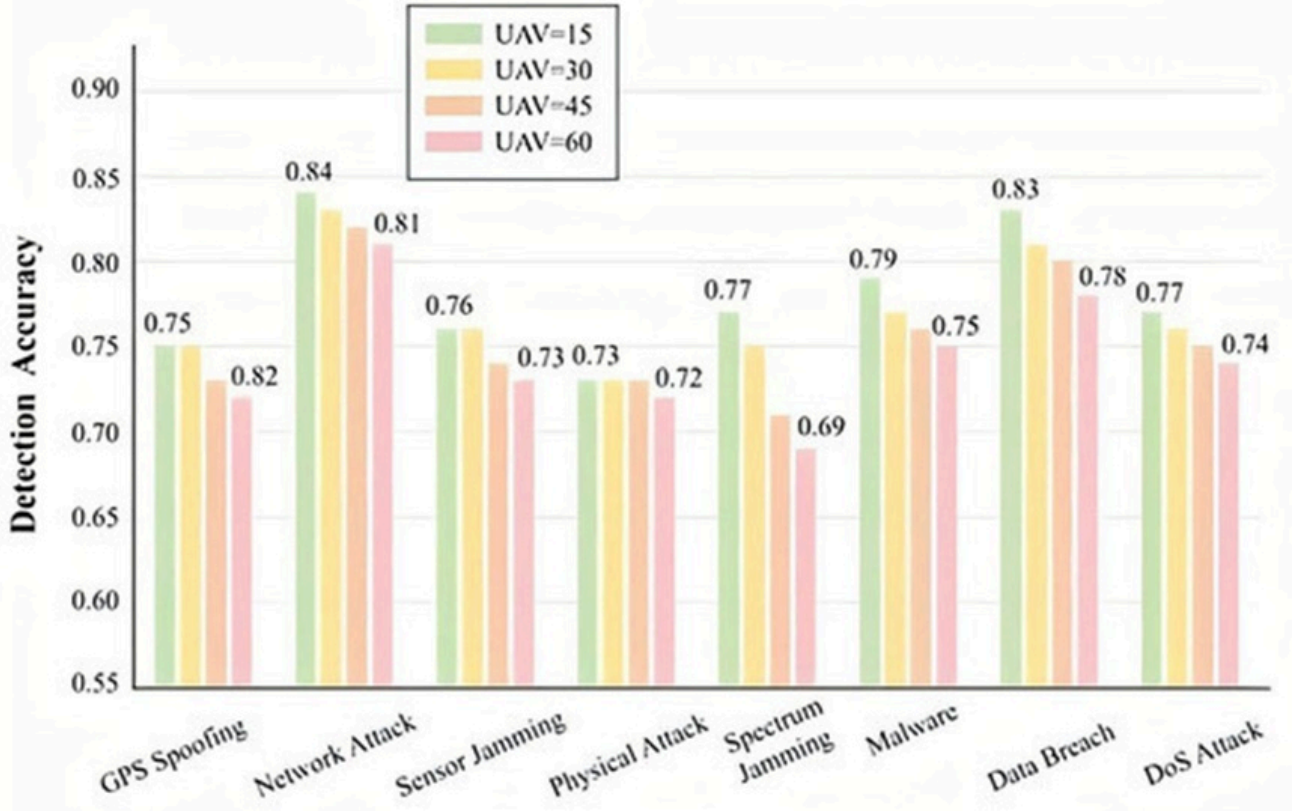
Figure 15. Threat type detection accuracy (UAV = 16).

We selected GNN, which exhibited standout results among the comparator algorithms, for contrastive scrutiny. We analyzed the accuracy trajectories alongside LLM-LCSA across varying UAV counts, as shown in **Figure 16**. Physical strikes usually carry severe repercussions, are comparatively easy to detect, and their accuracy remains largely indifferent to UAV scale variation. For network strikes, attack sources can branch out through numerous channels. Even a single strike readily detectable in compact networks may transmute into a hard-to-trace “multi-point synchronized assault” in vast networks. Consequently, as the UAV node count increases, the accuracy of network strike-detection algorithms tends to erode. Nonetheless, LLM-LCSA maintains an accuracy exceeding 80%, demonstrating pronounced robustness. Although GNN techniques are theoretically suited to networked configurations, their performance likewise falters when grappling with large-scale, high-density graph architectures due to computational complexity strains. Notably, despite this performance erosion, LLM-LCSA retains the highest absolute accuracy among all techniques across scales. Its performance erosion is comparatively subdued, far less drastic than that observed in baseline techniques.

© 2023 The Author(s). | Published by Agro Intelligence Research Press



(a) Threat detection accuracy of LLM-LCSA.



(b) Threat detection accuracy of GNN.

© 2023 The Author(s). | Published by Agro Intelligence Research Press

Figure 16. Threat detection accuracy of LLM-LCSA and GNN.

To situate this inquiry within the broader realm of large-scale parallel and clustered systems, we place it alongside pioneering work in the field of cluster robotics to establish its position there. Yasser *et al.* [40] maximized task distribution efficiency by optimizing the communication topology within the cluster (CDTA-CL/DL), focusing on streamlining information flow pathways. The present study grapples with the unique security challenges of UAV clusters by advancing the LLM-LCSA architecture, shifting its emphasis to streamlining cognitive and decision-making pipelines. We deploy LLMs and MoEs mechanisms via a cloud–edge–end tiered structure, elastically marshaling expert knowledge to fend off complex threats while explicitly encoding resource bounds into the decision process. Hence, for tasks with well-defined contours, communication refinement stands as the method of choice; whereas for high-uncertainty challenges such as security, augmenting the system's cognitive intelligence becomes essential. Despite disparate paths, both reinforce a core axiom: efficient parallel systems depend on deliberate trade-offs between performance and resources inside decentralized coordination frameworks. Our work shows that this axiom extends from communication strata to AI decision strata, further validating the merit of LLM-LCSA within generalized parallel intelligent systems.

Conclusion

To address the difficulties conventional techniques face in multi-unit cooperative protection for UAV swarms—including dynamic threat proliferation, heterogeneous data integration challenges, and resource-constrained decision-making lag—this paper proposes LLM-LCSA. Through cloud–edge–end cooperative placement and intelligent agent decision-making, the proposed framework provides an effective countermeasure against threats. The core contributions of this investigation are outlined below.

We propose the LLM-LCSA model, which interlinks short- and long-range historical databases via a sliding-window integration scheme to boost the throughput of multisource asynchronous data merging. Every constituent garners robust performance scores. In addition, we introduce hybrid expert-based intelligent agents and engineer a tiered cooperative threat identification algorithm, achieving a mean gain of 7.92% in threat identification accuracy over conventional techniques. In resource-constrained settings, we formulate a multi-objective optimization model that balances resource consumption and performance, effectively reducing communication burden and decision lag. The simulation results show a 44.52% reduction in total decision time compared to conventional techniques. The load distribution tactic successfully circumvents single-resource chokepoints, significantly elevating resource efficiency.

This paper provides a novel solution to the cooperative protection of UAV swarms. Future explorations will build on this foundation to strengthen the practicality and scalability of LLM-LCSA. Key directions include investigating lightweight models for physical-layer strike identification, designing a cross-swarm federated learning framework for privacy-protective cooperative training, and verifying the system's real-time behavior within converged 6G network settings, such as highly secure smart factories, low-latency smart cities, and data-sharing smart logistics.

Abbreviations

The following abbreviations are used in this manuscript:

BS	Base station
CPU	Central processing unit
DoS	Denial of service
GCS	Ground control station
GPS	Global positioning system

© 2023 The Author(s). | Published by Agro Intelligence Research Press

GSK	Group secret key
IAB	Integrated access and backhaul
KKT	Karush–Kuhn–Tucker
LLM	Large language model
LoS	Line-of-sight
MoEs	Mixture of experts
NLoS	Non-line-of-sight
RAG	Retrieval-augmented generation
RAM	Random access memory
SDN	Software-defined networking
UAV	Unmanned Aerial Vehicle
V2X	Vehicle-to-everything

Acknowledgements

None

Conflict of interest

None

Financial support

This work was supported by the National Key Research and Development Program of China under Grant 2024YFE0200300, the National Natural Science Foundation of China (No. 92367201 and No. 62371039), and BIT Research and Innovation Promoting Project (Grant No. 2024YCXY027).

Ethics statement

None

Received: 27 Jun 2022 Revised: 01 Sep 2022 Accepted: 16 Sep 2022
Published online: 25 November 2023

Rights and permissions

Open Access The author(s) retain copyright. This article is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License. It may be shared and adapted for non-commercial purposes with appropriate attribution, an indication of changes, and distribution of adaptations under the same license. Third-party material may be subject to separate terms identified in its credit line. View the license at https://creativecommons.org/licenses/by-nc-sa/4.0/.

References

1. Boroujeni SPH, Razi A, Khoshdel S, Afghah F, Coen JL, O'Neill L, et al. A comprehensive survey of research towards AI-enabled unmanned aerial systems in pre-, active-, and post-wildfire management. Inf Fusion. 2024;108:102369.

2. Nahiyoon SA, Ren Z, Wei P, Li X, Li X, Xu J, et al. recent development trends in plant protection UAVs: A journey from conventional practices to cutting-edge technologies—a comprehensive review. Drones. 2024;8:457.

3. Mendu B, Mbuli N. State-of-the-Art review on the application of unmanned aerial vehicles (uavs) in power line inspections: Current innovations, trends, and future prospects. Drones. 2025;9:265.

4. Betti Sorbelli F. UAV-Based delivery systems: A systematic review, current trends, and research challenges. ACM J Auton Transport Syst. 2024;1:1-40.

5. Wang X, Zhao Z, Yi L, Ning Z, Guo L, Yu FR, et al. A Survey on security of uav swarm networks: Attacks and countermeasures. ACM Comput Surv. 2025;57:1-37.

6. Kerns AJ, Shepard DP, Bhatti JA, Humphreys TE. Unmanned aircraft capture and control via gps spoofing. J Field Robot. 2014;31:617-36.

7. Ko Y, Kim J, Duguma DG, Astillo PV, You I, Pau G. Drone secure communication protocol for future sensitive applications in military zone. Sensors. 2021;21:2057.

8. Ashraf SN, Manickam S, Zia SS, Abro AA, Obaidat M, Uddin M, et al. IoT empowered smart cybersecurity framework for intrusion detection in internet of drones. Sci Rep. 2023;13:18422.

9. Tan YH, Lai S, Wang K, Chen BM. Cooperative control of multiple unmanned aerial systems for heavy duty carrying. Annu Rev Control. 2018;46:44-57.

10. Raja G, Senthivel SG, Balaganesh S, Rajakumar BR, Ravichandran V, Guizani M. MLB-IoD: Multi layered blockchain assisted 6g internet of drones ecosystem. IEEE Trans Veh Technol. 2023;72:2511-20.

11. Karmakar R, Kaddoum G, Akhrif O. A Blockchain-Based distributed and intelligent clustering-enabled authentication protocol for uav swarms. IEEE Trans Mob Comput. 2024;23:6178-95.

12. Jangsher S, Al-Dweik A, Iraqi Y, Pandey A, Giacalone JP. Group secret key generation using physical layer security for uav swarm communications. IEEE Trans Aerosp Electron Syst. 2023;59:8550-64.

13. Viana J, Farkhari H, Sebastião P, Campos LM, Koutlia K, Bojovic B, et al. Deep attention recognition for attack identification in 5g uav scenarios: novel architecture and end-to-end evaluation. IEEE Trans Veh Technol. 2024;73:131-46.

14. Lopez MA, Baddeley M, Lunardi WT, Pandey A, Giacalone JP. Towards Secure Wireless Mesh Networks for UAV Swarm Connectivity: Current Threats, Research, and Opportunities. In: Proceedings of the 2021 17th International Conference on Distributed Computing in Sensor Systems (DCOSS). Pafos, Cyprus; 2021:319-26.

15. Jalil Hadi H, Cao Y, Li S, Hu Y, Wang J, Wang S. Real-Time Collaborative Intrusion Detection System in UAV Networks Using Deep Learning. IEEE Internet Things J. 2024;11:33371-91.

16. Hadi HJ, Cao Y, Khan MK, Ahmad N, Hu Y, Fu C. UAV-NIDD: A dynamic dataset for cybersecurity and intrusion detection in uav networks. IEEE Trans Netw Sci Eng. 2025;12:2739-57.

17. Yang Z, Zhang Y, Zeng J, Yang Y, Jia Y, Song H, et al. AI-Driven safety and security for uavs: From machine learning to large language models. Drones. 2025;9:392.

© 2023 The Author(s). | Published by Agro Intelligence Research Press

18. Javaid S, Fahim H, He B, Saeed N. Large language models for uavs: current state and pathways to the future. IEEE Open J Veh Technol. 2024;5:1166-92.

19. Liu L, Li W, Zhou F. Enhancing 6G iot communications: uav relayed satellite d2d with large language model optimization. IEEE Commun Mag. 2025;63:90-6.

20. Aikins G, Dao MP, Moukpe KJ, Eskridge TC, Nguyen KD. LEVIOSA: natural language-based uncrewed aerial vehicle trajectory generation. Electronics. 2024;13:4508.

21. Li H, Xiao M, Wang K, Kim DI, Debbah M. Large Language Model Based Multi-Objective Optimization for Integrated Sensing and Communications in UAV Networks. arXiv. 2024;arXiv:2410.05062.

22. Han B, Chen Y, Li J, Li J, Su J. SwarmChain: Collaborative LLM inference for uav swarm control. IEEE Internet Things Mag. 2025;8:64-71.

23. Zhu B, Bedeer E, Nguyen HH, Barton R, Gao Z. UAV trajectory planning for aoi-minimal data collection in uav-aided iot networks by transformer. IEEE Trans Wirel Commun. 2023;22:1343-58.

24. Emami Y, Zhou H, Nabavirazani S, Almeida L. LLM-Enabled in-context learning for data collection scheduling in uav-assisted sensor networks. IEEE Internet Things J. 2025;1.

25. Golam M, Alam MM, Kim DS, Lee JM. BLM-Chain: AI-Driven Blockchain for UAV Threat Resistance in IoBT. In: Proceedings of the 2024 15th International Conference on Information and Communication Technology Convergence (ICTC). Jeju Island, Republic of Korea; 2024. p. 1609-13.

26. Piggott B, Patil S, Feng G, Odat I, Mukherjee R, Dharmalingam B, et al. Net-GPT: A LLM-Empowered Man-in-the-Middle Chatbot for Unmanned Aerial Vehicle. In: Proceedings of the Eighth ACM/IEEE Symposium on Edge Computing. Wilmington, DE, USA; 2023. p. 287-93.

27. Sezgin A. Scenario-Driven evaluation of autonomous agents: integrating large language model for uav mission reliability. Drones. 2025;9:213.

28. Zhou Q, Wu J, Zhu M, Zhou Y, Xiao F, Zhang Y. LLM-QL: A LLM-enhanced q-learning approach for scheduling multiple parallel drones. IEEE Trans Knowl Data Eng. 2025;37:5393-406.

29. Usman M, Amin R, Aldabbas H, Alouffi B. lightweight challenge-response authentication in sdn-based uavs using elliptic curve cryptography. Electronics. 2022;11:1026.

30. Mughal UA, Hassler SC, Ismail M. Machine Learning-Based Intrusion Detection for Swarm of Unmanned Aerial Vehicles. In: Proceedings of the 2023 IEEE Conference on Communications and Network Security (CNS). Orlando, FL, USA; 2023:1-9.

31. Deng H, Lu Y, Yang T, Liu Z, Chen J. Unmanned Aerial Vehicles anomaly detection model based on sensor information fusion and hybrid multimodal neural network. Eng Appl Artif Intell. 2024;132:107961.

32. Masadeh A, Alhafnawi M, Salameh HAB, Musa A, Jararweh Y. Reinforcement learning-based security/safety uav system for intrusion detection under dynamic and uncertain target movement. IEEE Trans Eng Manag. 2024;71:12498-508.

33. Li J, Sun G, Duan L, Wu Q. Multi-Objective optimization for uav swarm-assisted iot with virtual antenna arrays. IEEE Trans Mob Comput. 2024;23:4890-907.

34. Zhai W, Liu L, Ding Y, Sun S, Gu Y. ETD: An efficient time delay attack detection framework for uav networks. IEEE Trans Inf Forensics Secur. 2023;18:2913-28.

© 2023 The Author(s). | Published by Agro Intelligence Research Press

35. Tlili F, Ayed S, Fourati LC. A new hybrid adaptive deep learning-based framework for uavs faults and attacks detection. IEEE Trans Serv Comput. 2023;16:4128-39.

36. Ding Y, Zhang Q, Lu W, Zhao N, Nallanathan A, Wang X, et al. Collaborative communication and computation for secure uav-enabled mec against active aerial eavesdropping. IEEE Trans Wirel Commun. 2024;23:15915-29.

37. Hao JX, Chen L, Meng L. Advancing large language models with enhanced retrieval-augmented generation: Evidence from biological uav swarm control. Drones. 2025;9:361.

38. El Alami H, Rawat DB. Lightweight Language Models in Autonomous Systems: In-Context Learning with Bidirectional Alignment for Fault Detection. In: Proceedings of the ICC 2025—IEEE International Conference on Communications. Montreal, QC, Canada; 2025. p. 4395-400.

39. Yan W, Sun H, Zhang X, Liang X, Zhu S, Jiang Z. Boosting resilience design of cargo UAVs: A fault diagnosis method utilizing MRKG and LLM-FCT reasoning. J Eng Des. 2025;1-27.

40. Yasser M, Shalash O, Ismail O. Optimized decentralized swarm communication algorithms for efficient task allocation and power consumption in swarm robotics. Robotics. 2024;13:66.

© 2023 The Author(s). | Published by Agro Intelligence Research Press