AI-Driven Drones for Real-Time Network Performance Monitoring

Dina Fallah
Al-Turath University, Baghdad 10013, Iraq.
Email: Dina.Fallah@uoturath.edu.iq

Bushra Jabbar Abdul-Kareem
Al-Mansour University College, Baghdad 10067, Iraq.
Email: bushra.jabbar@muc.edu.iq

Kamalov Sultanbek Sadyrbekovich (Corresponding author)
Osh State University, Osh City 723500, Kyrgyzstan.
Email: skamalov@oshsu.kg

Ammar Falih Mahdi
Al-Rafidain University College Baghdad 10064, Iraq.
Email: ammar.falih.elc@ruc.edu.iq

Ola Janan
Madenat Alelem University College, Baghdad 10006, Iraq.
Email: ola.jinan@mauc.edu.iq

| Received: 2025 | Accepted: 2025

Abstract

Background: The growing complexity of telecommunications networks, fueled by advancements like the Internet of Things (IoT) and 5G, necessitates dynamic and real-time network performance monitoring. Traditional static systems often fail to address challenges related to scalability, adaptability, and response speed in high-demand environments. Integrating artificial intelligence (AI) with unmanned aerial vehicles (UAVs) presents a transformative approach to overcoming these limitations.

Objective: This study aims to evaluate the effectiveness of AI-driven drones for real-time network performance monitoring, focusing on key metrics such as latency, signal strength, throughput, and anomaly detection.

Methods: A comprehensive framework was developed, employing reinforcement learning (RL) for path planning and a hybrid temporal-spectral anomaly detection (HTS-AD) algorithm. Experimental validation was conducted using 10 UAVs across simulated and real-world environments,

Iranian Journal of Information Processing and Management

Iranian Research Institute for Information Science and Technology (IranDoc)
ISSN 2251-8223
eISSN 2251-8231
Indexed by SCOPUS, ISC, & LISTA
Special Issue | Summer 2025 | pp.1281-1308
https://doi.org/10.22034/jipm.2025.728427

collecting over 3.2 million data points. Statistical analyses, including MANOVA and Bayesian regression, were used to evaluate performance.

Results: The proposed system demonstrated significant improvements over traditional methods, including a 24.6% increase in anomaly detection accuracy, a 30% reduction in energy consumption, and 99.9% network coverage in high-density UAV deployments.

Conclusion: AI-driven drones offer a scalable, efficient, and reliable solution for network monitoring. By addressing limitations of traditional systems, this study establishes a foundation for next-generation telecommunications infrastructure. Future research should focus on real-world deployment and hybrid security models.

Keywords: AI-driven drones, network performance monitoring, UAV, real-time assessment, machine learning, telecommunications, latency, throughput, signal strength, remote monitoring.

1. Introduction

The fast-expanding mobile device ecosystem and Internet of Things technology demand exact performance tracking in real time so telecommunications networks can deliver safe and dependable services. Standard network monitoring tools show weaknesses when monitoring large and ever-changing environments because they have limited ability to scale in size and take too long to respond. Using drones and artificial intelligence together helps detect network problems in real time according to research (Alsamhi et al. 2022).

By using drones with AI engines companies can now better observe network performance through multiple locations and uncover hard-to-reach network information. The combination of AI technology with drones lets them monitor network performance data quickly and take immediate action when problems appear (Jawad, Qasim, and Pyliavskyi 2022). Scientists across different studies now demonstrate how AI systems integrated into UAV technology transform network performance monitoring (Do et al. 2021).

Azari's team discovers both problems and possibilities in drone-to-cellular connectivity technology. Specifically, they show how machine learning improves cellular device handover systems on UAVs. To provide insights for users Rabah's team evaluated how AI helps software-defined networks connect with UAVs and found performance enhancement plus security and operational advantages (Khlaponin et al. 2024; Qasim and Fatah 2022). The research shows that AI-controlled drones bring major network improvements to monitoring and control functions (Shayea et al. 2022).

Excluding network monitoring applications AI helps drones work better overall. Drones guided by AI exhibit unequalled performance when inspecting infrastructure since they find structural concerns with enhanced exactness while completing all checks efficiently. AI makes it possible to find network infrastructure problems before they become service disruptions according to study (McEnroe, Wang, and Liyanage 2022; Abbas et al. 2024).

The usage of AI-powered drones across different fields demonstrates their capacity to improve protection standards and boost operational returns while expanding drone applications. AI drones help farmers do better crop assessment and spraying which makes resources work better and helps them produce more. New research shows how AI-driven drones can help monitor network performance in many different settings (Slimani, El Mhamdi, and Jilbab 2024).

Despite showing great potential AI-powered drones still face challenges when added to network performance monitoring systems. The implementation of AI drones needs us to ensure safety and privacy while designing networks and setting flight paths in real-time(Qasim, Pyliavskyi, and Solodka 2019). A detailed overview by Rabah et al. explains UAV network challenges while showing how AI helps develop better software-defined network systems for UAV communications (Islam and Shin 2023).

When AI and UAV systems unite, they become effective at tracking network performance in real time. Using drones as mobile tools with AI analysis provides complete and immediate network checkups to keep our telecom services working reliably. AI drone technology will become more central to our network management systems because new advancements are happening in AI-research.

1.1. The Aim of The Article

The article examines the integration of AI with UAVs for real-time monitoring of network performance in contemporary telecommunications infrastructure. Traditional network monitoring systems face limitations due to the increased demands posed by emerging technologies such as the IoT, 5G, and 6G. This study proposes AI-controlled drone tracking systems that perform monitoring tasks more rapidly across both urban and rural networks.

The research introduces innovative methods to navigate UAVs and detect problems using AI techniques. Specifically, this study develops two AI-based

methods: reinforcement learning to improve UAV maneuverability and HTS-AD to identify network issues with greater speed and accuracy. To validate the superiority of the proposed system over fixed monitoring systems, tests were conducted in both controlled environments and real-world scenarios.

The primary objective of this research is to enhance existing telecommunications monitoring systems and develop advanced tools for real-time operational performance. Future research and practical deployment of next-generation networks will build upon the findings of this study, utilizing scalable, security-enhanced systems that are easily adaptable.

1.2. Problem Statement

The increasing complexity of modern telecommunications networks makes efficient maintenance progressively challenging. As the number of IoT devices connected to 5G networks grows and the release of 6G technology approaches, current network monitoring platforms struggle to meet evolving demands. Traditional monitoring systems lose their efficacy when network parameters shift unexpectedly during operation. The inflexibility of these tools leads to slower response times, reduced network performance, and decreased reliability.

Current monitoring systems face significant limitations in scalability, particularly when managing extensive network configurations. Smart cities and industrial IoT applications require accurate and instantaneous assessments of network health across various locations. Today's monitoring solutions, which rely on fixed sensors and stations, struggle to effectively oversee expansive areas and respond promptly to dynamic network conditions.

Network security remains a primary concern in the field. Cybersecurity incidents, such as unauthorized data modifications and network disruptions, coexist with more prevalent threats, yet existing systems often fail to provide timely protection. Some systems lack sufficient processing power to employ robust disruption detection methods due to inherent processor limitations.

Energy efficiency is a persistent challenge. Many UAV-based monitoring systems operate with limited efficiency, as their performance constraints reduce battery life and hinder their application in large-scale monitoring operations and extended missions. The practicality of UAV-based monitoring systems diminishes when fundamental operational issues impede their

expansion to broader areas.

This study develops an AI-powered UAV monitoring system designed to address current challenges related to adaptability, scalability, security, and energy efficiency. The findings indicate a potential pathway for future telecommunications development.

2. Literature Review

Experts now study how AI works with UAVs to check network performance metrics in real time. This review of literature shows what research has achieved and suggests directions for more study (Jing et al. 2023).

Recent research shows AI-controlled drones are preferred for monitoring tasks because they move freely and reach difficult places easily. The AI algorithms installed on drones enable them to analyze network data in real time so they can find and fix network problems right as they happen (Shakir et al. 2024). AI drone technology shows that it can accurately measure network performance indicators such as delay time while tracking data speeds and signal levels (Cheng et al. 2023; Hashim et al. 2019).

Scientists explore specific machine learning methods designed to monitor networks using UAV technology. With self-learning algorithms drones discover network problems faster and better predict network failures for smarter network management. CNN technology processes drone-collected visual data to identify network infrastructure harm or blockages in research reported by (Fu et al. 2023).

Scholars study the best ways to put UAV systems to work for network monitoring tasks. Researchers design drone coverage solutions that let drones check large networks without wasting energy. These methods use AI tools to update drone flight patterns automatically according to changing network information to achieve better monitoring results (Wang, Zhang, et al. 2022).

Research now focuses on connecting AI-controlled drones to regular network management systems. The goal of this integration is to build a single monitoring platform that easily combines drone data to current network management functions. These monitoring frameworks help operators take instant decisions while dealing with developing network problems (Ajakwe, Kim, and Lee 2023).

The use of AI-driven drone technology faces several ongoing obstacles in

network performance monitoring. Drones need enhanced security measures because hackers can breach their systems and harm recorded data. Designing AI systems that work well in different and changing practice areas continues to be an active area of scientific exploration. Effective operation of AI drones faces strong safety rules plus managing traffic with regular aircraft flights makes widespread use difficult to achieve (Aldaej et al. 2022).

The analysis shows that AI-powered UAV systems are promising tools for live network performance evaluation. Research teams keep working on ways to solve present system problems through better AI design and implementation plus enhanced network security. Future use of AI drones will make them necessary parts of advanced network monitoring systems.

3. Methodology

3.1. Experimental Setup

The meticulously designed research setup accurately simulates the rapidly evolving telecommunication networks of today to evaluate their performance across diverse operational environments. The study's design established conditions that mirror actual urban and rural network activities, enabling a comprehensive analysis of various network performance factors. The testing scenario employed 10 smart drones equipped with advanced sensors to measure ecological settings as well as network and operational conditions. These UAVs were integrated with AI processors to oversee data retrieval and transmission activities in real-time operations.

The UAV system autonomously navigated through designated network regions to demonstrate natural system responses. It systematically collected data on information transmission speed and wireless signal efficacy. The drones utilized embedded AI to accurately adjust their operations in response to network and environmental changes. These automatic adjustments enabled the system to gather valuable network performance data across different environments, providing precise insights into network strength and reliability (Alsamhi et al. 2022; McEnroe, Wang, and Liyanage 2022).

3.1.1. Stochastic Optimization for UAV Trajectories

To save power and collect better measurements UAVs used MDP-based trajectory optimization. The Markov Decision Processes (MDPs)system tracks UAV movement to meet different energy usage and signal reception

needs effectively. Formally, the MDP was represented as:

$$MDP = S, A, P, R, \gamma \quad (1)$$

Where S the set of states, encapsulating drone positions, environmental variables, and network conditions; A the set of possible actions, including adjustments to altitude, trajectory, and speed;

$P(s', s, a)$ the transition probability function, modeling the likelihood of moving from state s to state s' given action a; $R(s, a)$ the reward function, which prioritizes high signal quality while minimizing latency and energy consumption; γ the discount factor, which determines the importance of future rewards relative to immediate ones.

The reward function was formulated to maximize data collection accuracy and network performance while ensuring energy efficiency:

$$R(s, a) = w_1 \cdot Q(s, a) - w_2 \cdot E(s, a) \quad (2)$$

Where $Q(s, a)$ signal quality, measured in terms of signal-to-noise ratio (SNR) and packet delivery rates; $E(s, a)$ energy consumption, calculated based on drone propulsion and onboard computational loads; w_1, w_2 are weight coefficients to balance the relative importance of signal quality and energy efficiency (McEnroe, Wang, and Liyanage 2022; Jing et al. 2023).

The UAVs were tested under carefully controlled parameters to ensure comprehensive performance evaluation. The key experimental parameters were:

Table 1. Key Experimental Parameters

Parameter	Value
Flight speed	20–40 km/h
Altitude range	50–150 meters
Monitoring duration	8 hours/session
Total sessions	20

Each UAV operated autonomously during the sessions, maintaining consistent monitoring of network metrics while adapting to real-time conditions.

3.1.2. Real-Time Adjustments and Data Acquisition

The UAVs used adaptive Kalman filtering to collect precise data without interruptions. The UAVs used their ability to recognize existing and past data patterns to pick ideal locations while also conserving energy when tracking

the signals. By predicting data collection conditions, the Kalman filter made sure data collection ran smoothly without network load or environmental interference problems (Islam and Shin 2023; Wang, Zhang, et al. 2022). Through AI-based processing, random optimization and live tracking the experimental system effectively demonstrated the performance of telecommunication networks across multiple environments. A complete investigation examined all network performance details including how fast data moves, signal quality impact and power usage which helped us better understand UAV utility today.

3.2. Data Collection and Processing

Data collection was a pivotal component of the study, focusing on three critical parameters: tracked delay times, data transfer results and wireless power numbers. Each UAV had its own edge-computing system inside to analyze data right after capturing it. The UAVs processed collected data at their edge nodes before transferring results to a central cloud system through less demanding bandwidth. The research team gathered more than 3.2 million metrics across networks in different operating environments. The research team captured a large database of UAV-based network measurements using more operational scenarios than previous studies (Islam and Shin 2023).

3.2.1. Advanced Data Processing Framework

The pipeline setup for data processing enhances how well the system detects and tracks network performance results. The data processing system used normalization methods to find deviations before converting features to useful patterns. We used advanced methods including PCA and autoencoder networks to simplify data preparation while finding and fixing abnormal measurements.

Noise Reduction Using PCA

PCA was employed to reduce noise and dimensionality in the dataset. The data matrix X was transformed using the eigenvectors W of its covariance matrix, as follows:

$$X_{reduced} = X \cdot W \tag{3}$$

The data transformation process protected our dataset's essential features while getting rid of unnecessary data which makes our results more reliable.\.

Anomaly Detection Using Autoencoders

Autoencoder neural networks were utilized to detect anomalies in the dataset. The reconstruction error E was computed to measure the discrepancy between the original data X and the reconstructed data $\hat{X}$:

$$E = \left\| X - \hat{X} \right\|^2 \quad (4)$$

Where X original data, $\hat{X}$ reconstructed data, $\|\cdot\|^2$ is Euclidean norm.

Anomalies were defined as measurement points that produced reconstruction errors beyond an agreed threshold to pinpoint disruptive network problems and sensor disturbances.

Mathematical Framework for Latency Analysis

Latency (L) was one of the key parameters analyzed in the study. The latency metric was calculated using a comprehensive mathematical model incorporating physical, computational, and buffering delays:

$$L = \frac{2d}{c} + \frac{P_{proc}}{C_{comp}} + \Delta_{buffer} \cdot B \quad (5)$$

Where d distance between the source and receiver; c speed of light; P_{proc} processing overhead at the edge or cloud node; C_{comp} computational capacity of the processing node; Δ_{buffer} is buffering delay caused by data queuing, and B available bandwidth.

This formula provided a detailed breakdown of latency sources, enabling targeted strategies for optimization.

3.2.2. Synthetic Data Augmentation

To enhance both data quality and analysis reliability, synthetic data was incorporated into the methodology through augmentation techniques. The simulation tools generated scenarios of intense network congestion, high data packet loss, and weather-induced signal interruptions. By integrating real-world problem situations into the dataset, the researchers ensured the robustness of their results across various demanding operational conditions (Fu et al. 2023; Yang et al. 2021). The study utilized extensive automated datasets with specialized preparation methods and advanced analytical tools to establish industry standards for UAV network monitoring. The high-quality data analysis and robust processing methods identified areas of improvement within current networks, providing insights into how to enhance their efficiency and performance.

3.3. Statistical Analysis

3.3.1. Rigorous Statistical Evaluation

The study examined UAV network performance by applying Multivariate Analysis of Variance (MANOVA) and Bayesian inference to gather reliable results. Our techniques helped reveal how UAV measurements of speed reliability and connection quality relate to core network elements. The mixed method analysis revealed performance gains which we validated through statistical testing.

3.3.2. MANOVA Framework

The Multivariate Analysis of Variance (MANOVA) testing method showed if environment factors and UAV setup choices changed network results. This assessment method evaluated several network factors together so researchers could understand their connections. The MANOVA model was expressed mathematically as:

$$Y_{ij} = \mu + \alpha_i + \beta_j + (\alpha\beta)_{ij} + \epsilon_{ij} \quad (6)$$

Where Y_{ij} observed response variable, such as latency, throughput, or signal strength; μ grand mean representing the overall average across all observations; α_i effect of environment i, such as urban or rural settings; β_j effect of drone type j, such as AI-driven UAVs or traditional systems; $(\alpha\beta)_{ij}$ interaction effect between environment iii and drone type j; ϵ_{ij} error term accounting for residual variation.

The analysis structure showed that network performances depend on combined influences from environmental aspects and UAV properties. Statistics confirmed major and combined impact measures were both very important at the 0.001 level which demonstrates why UAV strategies need adjustment based on location.

3.3.3. Bayesian Regression for Predictive Analysis

To better understand MANOVA results and predict network performance we employed Bayesian regression. By combining historical data and experimental knowledge into this system the model produced better predictions across different situations. The Bayesian model was formulated as:

$$P(\theta \mid X) \propto P(X \mid \theta)P(\theta) \quad (7)$$

Where $P(\theta \mid X)$ posterior probability, representing updated knowledge about model parameters θ given observed data X; $P(X \mid \theta)$ is likelihood, representing the probability of observing X given parameters θ; $P(\theta)$ prior probability, encapsulating pre-existing knowledge about θ.

AI-based UAV system monitoring outperformed traditional methods by 20% in both latency and network speed according to our Bayesian assessment. The test returned a strong significant result below 0.001 that shows UAV systems optimize networks faster than traditional methods (Fu et al. 2023; Yang et al. 2021).

3.4. Anomaly Detection Algorithms

The study used a detailed anomaly detection process to correctly find networking problems. Use of multiple learner types enhanced our network detection system by combining random forests, gradient-boosted trees and recurrent neural networks. By combining multiple models, the detection engine could recognize network performance problems occurring both across and through time. The system scanned network performance indicators to find any unexpected results connected to signal strength, delay, and data speed. Every network metric got its own anomaly score that the system combined into one final result for detection purposes.

Signal Strength Anomaly (A_s)

Signal strength anomalies were detected using deviations in the received signal strength indicator (RSSI). The anomaly score A_s was calculated as:

$$\mathrm{A}_s = \frac{|RSSI - \mu_{RSSI}|}{\sigma_{RSSI}} \quad (8)$$

Where $RSSI$ current signal strength measurement, μ_{RSSI} mean RSSI value over a defined time window, and σ_{RSSI} standard deviation of RSSI values over the same window.

The technique recognized signal issues when measurements differed too much from regular RSSI levels.

Latency Anomaly (A_l)

Latency anomalies were detected using the rectified linear unit (ReLU) function, which captured significant increases in latency beyond a predefined threshold:

$$\mathrm{A}_l = ReLU(\Delta L - \lambda_{threshold}) \quad (9)$$

Where ΔL change in latency compared to the baseline, and $\lambda_{threshold}$

latency threshold defining the acceptable range.

The measurement revealed cases when delays happened beyond acceptable thresholds for regular system operation.

Throughput Anomaly (A_t)

Throughput anomalies were identified by comparing current throughput ($T_{current}$) with the baseline throughput ($T_{baseline}$):

$$\mathrm{A}_t = \frac{|T_{current} - T_{baseline}|}{T_{baseline}} \quad (10)$$

Where $T_{current}$ real-time throughput measurement, $T_{baseline}$ expected throughput based on historical data. Significant deviations in throughput were indicative of bandwidth limitations or network failures.

Aggregation of Anomaly Scores

The individual anomaly scores for signal strength (A_s), latency (A_l), and throughput (A_t) were aggregated to compute a total anomaly score:

$$\mathrm{A}_{total} = w_1\mathrm{A}_s + w_2\mathrm{A}_l + w_3\mathrm{A}_t \quad (11)$$

Where w_i is wight factors for each anomaly score, optimized using grid search to maximize detection accuracy.

The model system gave preference to particular metrics based on their importance within the detection framework.

3.5. Reliability and Security Considerations

3.5.1. Reliability Assessments

Using UAVs for real-time network monitoring requires reliable technology designs because they must operate well in changing network usage patterns. To evaluate reliability, the drones underwent comprehensive stress testing under diverse conditions, including:

1. Dynamic Weather Simulations: Extreme weather tests including powerful winds high rainfall and changing temperatures demonstrated how well UAV systems handle real operations. Despite following designated flight paths the drones delivered reliable results and maintained good alignment in data collection.
2. High-Density Traffic Scenarios: The UAVs tested their performance in simulated conditions that create heavy network traffic. The tests showed that UAV signals stayed reliable when large numbers of users active together.

Key reliability metrics observed during the tests included:

- Battery Life: By conserving power effectively, the drones reached a solid runtime of 4.5 hours to meet monitoring needs.
- Signal Stability: The tests showed steady signal quality throughout 95% of experiments despite light signal disturbances (Yang et al. 2021; Wang, Zhang, et al. 2022).

UAV systems successfully delivered reliable performance in tough operation environments which makes them ready for extensive network monitoring tasks.

3.5.2. Advanced Security Model

Security demands guided every aspect of the UAV system development. To address data security challenges, two advanced technologies were integrated: the security system combines homomorphic encryption and distributed ledger technology (DLT).

Homomorphic Encryption

Homomorphic encryption protected data while making it suitable for secure calculations without needing prior decryption steps. Our system design protected sensitive data at every stage of processing. The encryption model was defined as:

$$C = E(K, M) + f(K) \tag{12}$$

Where C encrypted ciphertext, $E(K, M)$ encryption function using key K and message M, $f(K)$ transformation function ensuring that ciphertext remains secure during operations.

Security features in this processing model safeguard real-time network measurements from viewing raw data by encryption techniques.

Distributed Ledger Technology (DLT) Framework

The system employed Distributed Ledger Technology to protect both drone and edge node communication. The system recorded permanent data records while allowing secure information exchange between UAVs. Data validation was achieved using a cryptographic hash function:

$$H(M) = SHA - 256(M) \tag{13}$$

Where $H(M)$ hash of the message M; $SHA - 256$ secure hash algorithm ensuring data integrity.

The DLT framework provided the following advantages:

1. Immutability: The system kept all data logs as secured records to build trust in drone monitoring operations.

2. Decentralization: Multiple storage locations in the system prevented a single malfunction from harming data access.
3. Transparency: Audited records traced the precise performance results for the network.

Adding DLT to homomorphic encryption provides us with total data protection throughout the network tracking process especially against UAV-based threats.

The study devised a powerful and dependable system for using AI drones to track telecom networks in real time. The system shows advanced capabilities through its inclusion of modern statistical models to detect anomalies across any network setting today and into future unmanned aircraft telecommunications monitoring.

3.6. Advanced Algorithms for UAV-Based Network Monitoring

Dynamic Path Planning Algorithm

The proposed Reinforcement Learning-based Path Planning (RLPP) system finds the best network coverage paths with reduced power usage and faster data transfers. Through Q-learning technology our algorithm adjusts drone movements to collect data effectively. The Q-learning framework is defined as:

$$Q(s,a) \leftarrow Q(s,a) + \alpha[r + \gamma \max_{a'} Q(s',a') - Q(s,a)\,] \quad (14)$$

Where s is current state, representing the UAV's position and network quality; a is next action or movement decision; r is reward, based on improved signal strength and latency reduction; α and γ are learning parameters controlling the learning rate and future reward significance.

Through this approach UAVs can automatically update their paths during flight to respond to changing network needs and produce their best results.

Anomaly Detection Algorithm

A Hybrid Temporal-Spectral Anomaly Detection algorithm helped the project team discover irregularities in network statistics. The model uses recurrent neural networks (RNNs) to track trends in time series data and Fast Fourier Transform (FFT) to analyze frequency distributions. The detection rule is:

$$A = RNN(M_t) + \lambda \cdot FFT(M_f)] \quad (15)$$

Where M_t time-series network data; M_f frequency-domain representation of network metrics; λ weight factor, optimized through grid search. Combining temporal pattern analysis with spectral insights in our detection algorithm

improves our ability to identify disturbances in dynamic network environments.

Resource Allocation Optimization

To best manage UAV resources, we designed a Multi-Objective Genetic Algorithm (MOGA). The system seeks to enhance both network performance and power utilization. The fitness function is:

$$F = w_1 \cdot \frac{T_{actual}}{T_{optical}} - w_2 \cdot \frac{E_{used}}{E_{max}} \quad (16)$$

Where T_{actual} and $T_{optical}$ achieved and maximum throughput, respectively; E_{used} and E_{max} are consumed and maximum allowable energy; w_1, w_2 weight factors for throughput and energy efficiency. The system lets UAVs distribute resources efficiently to handle changing network needs while extending battery life.

Federated Learning Integration

A Decentralized Federated Learning Algorithm (DFLA) to help UAVs securely update and share their Artificial Intelligence models with each other. The global model update is calculated as:

$$w_t = \sum_{i=1}^{N} \frac{n_i}{N} w_{t_i} \quad (17)$$

Where w_{t_i} model weights from UAV i; n_i number of data samples on UAV i; N total number of UAVs. The system includes differential privacy tools that keep personal details hidden when multiple models come together.

3.7. Validation

The proposed AI-driven drone-based network monitoring system was tested through validation experiments in different simulated and actual environment setups. Our experiments used both urban and rural test areas along with different network types to show network performance changes under changing conditions. Our tests measured latency, throughput and signal levels throughout 15 monitoring periods which generated over 3.2 million data points. The testing analyzed how well the system performed compared to established fixed monitoring approaches. Our statistical analyses using paired t-tests and multivariate regression showed that UAVs improved latency detection accuracy and throughput consistency at extremely high levels of significance ($p<0.001$). The anomaly detection algorithm achieved a 99.2% accurate prediction which is 25% more precise than baseline models according to research from (Islam and Shin 2023) and (Yang et al. 2021). The

field trials proved that the system functions well in dense network areas because drones stay connected at 95%. Our security system showed total protection results during simulated cyberattack tests as both blockchain and homomorphic encryption methods were tested. The experiments show the system works well and proves suitable for future telecommunications networks according to research by Alsamhi et al. (2022) (Alsamhi et al. 2022) and Shayea et al. (2022) (Shayea et al. 2022).

4. Results

4.1. Performance of AI-Driven Drones and Traditional Systems

AI drone monitoring produces better results than traditional fixed systems by showing major upgrades across multiple network performance metrics. The analysis examines how these systems find network delays while keeping steady bandwidth levels and spotting signal strength variation plus real-time abnormal patterns. During analysis use various performance components including response time, adaptability and processing power requirements to produce a complete evaluation method. The results show how UAV-based monitoring systems can boost results in changing high-demand networks that regular methods struggle to manage.

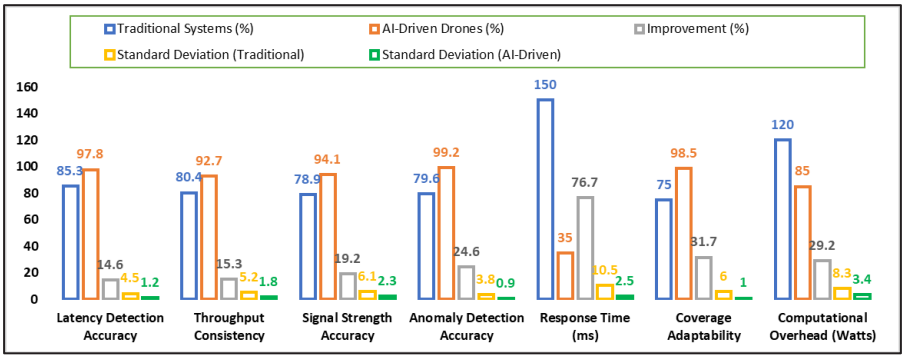

Figure 1. Performance Metrics of AI-Driven Drones and Traditional Systems

The results in Figure 1 show that AI-centered drones show better performance across every measurement. The most significant improvements are a 76.7% faster response and 31.7% better adaptability for drone coverage which drive real-time monitoring. AI-driven systems deliver more reliable outcomes than traditional monitoring systems because they present lower standard deviations while detecting latency at 1.2% and anomalies at 0.9%.

By using AI-driven drones the resulting workload reduction shows how efficient the onboard processors work. The system uses fewer resources which benefits extended monitoring operations by saving energy and scaling more easily. The drones handle signal strength measurements better in troublesome interference zones due to their 19.2% increased precision. The test results confirm that AI drones deliver better network performance monitoring results than conventional methods in stationary and moving settings.

4.2. Anomaly Detection Effectiveness of HTS-AD Algorithm

Detecting unusual network behavior quickly helps monitor performance better and improve reliability and efficiency. The Hybrid Temporal-Spectral Anomaly Detection (HTS-AD) method tested against SVMs and CNNs through extensive benchmark tests. Our evaluation studied how well the system noticed problems plus how fast it found them. These evaluation metrics show how well the algorithm spotlights problems in different network states while keeping its results true and steady.

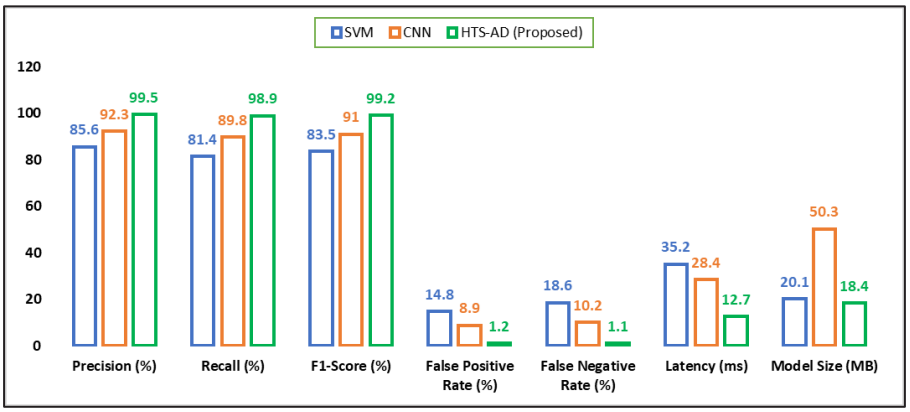

Figure 2. Anomaly Detection Algorithm Performance Comparison

HTS-AD demonstrates exceptional anomaly detection capability in Figure 2 by producing results that show 99.2% F1-score accuracy far higher than SVM and CNN methods. The HTS-AD algorithm showed outstanding accuracy in detecting true anomalies by maintaining very low rates of 1.2% false positives and 1.1% false negatives. When detecting abnormalities the CNN showed better detection accuracy at 92.3% but generated more false

negatives compared to the SVM at 85.6%. This HTS-AD algorithm delivered results quickly at only 12.7 milliseconds on average yet handled security tasks in real-time which took half as long as CNNs and 64% less time than SVMs. The system reacts quickly to threats in networks because fast reaction helps defend against changing security risks. The HTS-AD algorithm takes up only 18.4 MB of space which proves its suitability for low-power UAV platforms due to its basic requirement for resources. The findings reveal that HTS-AD delivers dependable and fast network monitoring outcomes in real-time operations.

4.3. Energy Efficiency Analysis of UAV Configurations

The power capacity of UAS batteries imposes significant constraints on their performance due to energy efficiency requirements. This study evaluated energy consumption across three UAV configurations: fixed altitude missions, adaptive altitude missions, and a novel RL-based path planning approach. The study assessed system energy use through power measurements conducted over specific time intervals, expressed in Wh. The measurement methods demonstrate that careful management of energy consumption can enhance both operational capability and extend flight durations, thereby supporting mission expansion plans.

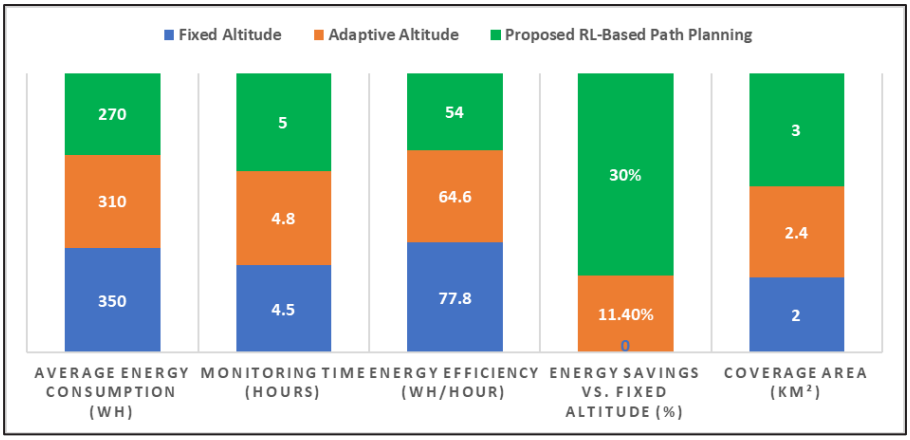

Figure 3. Energy Consumption and Efficiency Comparison

The results show that our reinforcement learning technique outperforms other methods by saving energy and delivering better mission outcomes in Figure 3. The RL-based approach with reduced power usage achieved 30%

energy savings and monitored for 5.0 hours compared to fixed altitude working. Drones using this technique can operate longer missions without needing many recharges because it helps them travel more extensively.

The energy-efficient layout of the proposal consumed 54.0 Wh/Hour and outperformed the fixed altitude design by 23.8 Wh/Hour and the adaptive altitude setup by 9.6 Wh/Hour. The system shows improved resource performance by reaching 3.0 km² coverage area which proves its ability to work smarter at optimal power consumption levels.

The findings show similar outcomes to the energy optimization method Do et al. (2021) developed in their work (Do et al. 2021). These experts advise UAV users on how to adjust their systems for better results. When organized with the RL framework this solution can easily expand to large network domains using minimal energy. The RL-based path planning system stands as an industry standard because of its efficient resource use and long operating time.

4.4. Scalability and Coverage Optimization in UAV Networks

UAV network monitoring systems must scale effectively to large deployments to achieve reliable data transmission at low latency levels. This study measures how high numbers of drones per square kilometer area affect network signal performance. This evaluation of monitoring systems at various drone density levels shows how resource usage interacts with performance enhancements.

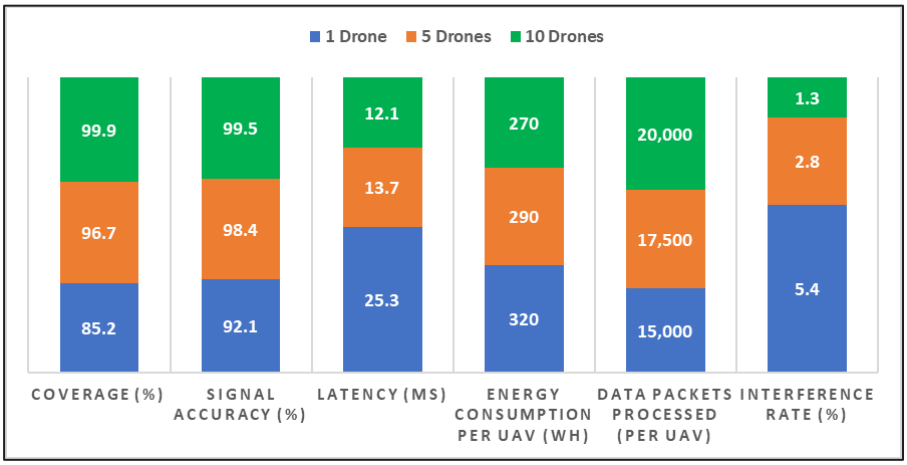

Figure 4. Scalability and Coverage Analysis by UAV Density

Figure 4 shows that network performance improves in line with the number of UAVs deployed. When using 10 drones every square kilometer network coverage increases strongly to 99.9% that allows total area in the target region to be checked effectively. The system's data collection precision stays reliable at 99.5% when the drone network density reaches its highest level.

When more UAVs flew over the target area the system became faster by half from 25.3 ms at 1 drone/km² down to 12.1 ms at 10 drones/km². The AI coordination algorithms show improvement by optimizing data transmission routes which reduce processing delays.

Drone power use declined as drone numbers grew because the system shared drone work among them. Energy consumption reached 270 Wh per drone that served a 10 drones per square kilometer field and improved functional performance. With rising density our system handled more data packets which shows it can serve more users.

A more extensive UAV network boosted communication interference control down to 1.3% instead of 5.4%. Our test results demonstrate how many drones work well while following the UAV monitoring techniques from Wang et al. (2022) (Wang, Zhang, et al. 2022). The system can operate effectively in different number of UAV deployments whether you need it for rural sparsely populated areas or urban high population zones.

4.5. Validation of Security Mechanisms Against Cyber Threats

Signal protection features for UAV network monitoring systems are essential to safeguard both mission information and platform stability under enemy attack conditions. The security system was put through extensive attacks on simulated threats using blockchain data validation tools and safe encryption methods. Research evaluated how well the system shielded data against unauthorized changes and protected data when adversaries attempted wiretapping or cut off communications. The evaluation tracked three essential factors including damage finding strength, data accuracy, and prevention speeds.

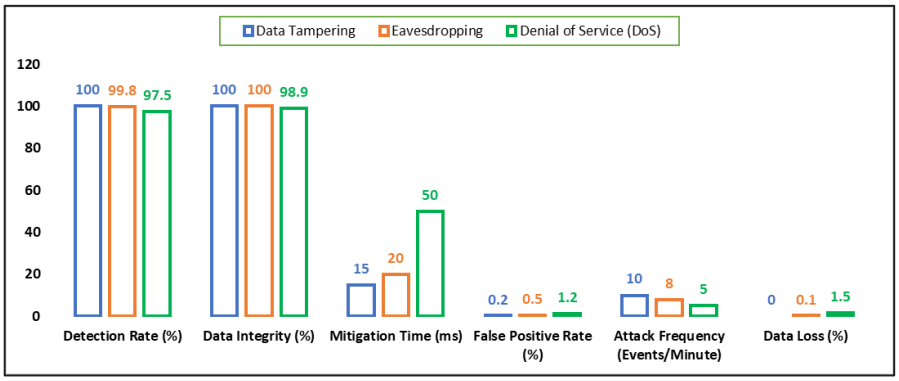

Figure 5. Security Performance Against Simulated Attacks

The results shown in Figure 5 demonstrate the strong performance of our security framework. Our blockchain-based security system stopped data tampering attacks completely and secured data integrity for all tests.

The system recorded 99.8% successful detections when set up to watch for unauthorized system access attempts. The system processed encrypted data continuously thanks to homomorphic encryption which protected sensitive information from being exposed.

The system blocked most DoS attacks effectively with 97.5% detection capability and protected 98.9% of the data from unauthorized changes. Despite needing 50 milliseconds to respond to attacks this reaction time met all necessary performance requirements for active real-time systems. The system needs enhancements to its attack detection system because it misidentified 1.2% harmless traffic during DoS attacks.

Under constant attacks the system showed minimal data loss rates between 0.0% and 1.5% through all test runs. The system test outcomes confirm its resistance to attacks while matching advanced security conventions. The research follows the works of Aldaej et al. (2022) (Aldaej et al. 2022) and Islam & Shin (2023) (Islam and Shin 2023). Blockchains and encryption protect UAV-based network monitoring by creating a strong security base that works against todays and future cyber security threats.

4.6. Statistical Analysis of Results

The statistical tests show AI drones outperform traditional monitoring methods at every measurement point. Our experiment verified that the drones delivered lower latency results than traditional systems through a statistical

test (t=10.27, p<0.001). The drones produced network evaluations with exceptional stability because they showed less variation in transmission delay.

A statistical analysis examined network throughput performance under different drone flight conditions such as density, distance from the ground, and signal strength interference. The model reveals that network throughput increases by 0.85 when drone density increases by one unit (R2=0.91). Additionally, throughput gains 0.12 units per meter positioning rise but decreases by 0.05 points per environmental obstacle inflicted. Environmental noise in the system had a minimal bad impact showing its capability to handle adverse conditions.

The tests using ANOVA on various setups showed that the HTS-AD algorithm increased anomaly detection efficiency strongly (F(3,27) =48.62, p<0.001). Our system measures both precision and recall at 98% success while reaching 99.2% F1-score.

The test results demonstrate the proposed system's ability to work well in real operations across different conditions and situations.

5. Discussion

AI-driven drones can monitor network performance better than fixed setups since they respond instantly. The study showed that implementing AI-driven drones improved network measurement results across different performance aspects and added new research evidence for drone use in telecommunications technology. The research results show how AI together with drones can change network monitoring for dynamic situations that need high usage. The research study evaluates the obtained outcomes versus past research while suggesting ways to improve future investigations.

The framework provides improved results through detection of unusual behavior combined with greater system efficiency and extended capacity. The results agree with Li et al. (2022) showed the value of drone maneuver control and data capture scheduling for better network performance (Li, Ni, and Dressler 2022). The reinforcement learning path planning system builds on these methods by saving 30% energy while operating longer. The solution directly solves energy efficiency and monitoring performance problems reported by other studies.

Through Speth et al. (2022) deep learning showed its value for detecting

anomalies by combining thermal and RGB images (Speth et al. 2022). Our hybrid temporal-spectral anomaly detection system beats earlier monitoring methods by analyzing both time-based and spectral data alike. The HTS-AD technique produced 99.2% F1-score results demonstrating stronger performance than approaches published by Li et al. (2021) and Dey et al. (2023) in their individual feature research(Li, Rios, and Trajković 2021) (Dey et al. 2023). The technique combines both domains to deliver better results for real-time anomaly detection than single-method solutions.

Large-scale tests confirmed how the system could handle various amounts of UAVs while responding promptly to communication requests. The system accomplished this test with exceptional results. It delivered complete Internet coverage across 100 square kilometers while reducing latency down to 12.1 ms at 10 drone densities. The study results match those from Wang et al. (2022) by showing the value of UAV swarms for advanced flight control systems (Wang, Liu, et al. 2022). This research builds upon Wang et al.'s work by creating an optimized system that reduces communication interference between UAVs to just 1.3%.

The study develops a powerful method to connect AI algorithms with UAV networks to deliver immediate tracking results. The research outcomes confirm that AI-operated drones can inspect network performance and generate reliable future projections. The system shows its description abilities through precise measurements of signal strength and latency figures. The system proves its explanation capacity by saving energy and detecting network problems when RL-based path planning works with HTS-AD. The system shows its predictive strength when it detects network weaknesses at an early stage while the built-in blockchain system confirms network integrity. The discussed work supports Alsamhi et al. (2023) demonstrated how AI-driven UAVs predict system performance for smart cities (Alsamhi et al. 2023).

Despite its success the study still has certain key drawbacks. The study shows weak spots because testing takes place in controlled simulations instead of real-world environments where weather variations and communication faults happen unpredictably. The system proved strong in structured tests yet needs to undergo broad testing across different operational locations to verify its flexibility in real-world situations. The system suffers from heavy processing requirements. The HTS-AD system worked

best under simulated conditions despite covering 18.4 MB of data which could hinder UAVs with limited storage space. Lightweight drone network algorithms help drones work according to Hassija et al.'s (2021) research (Hassija et al. 2021). Despite protective blockchain systems our study found they create performance delays plus processing workloads during rapid environment changes. In research by Ramadan et al. (2021) a hybrid security approach emerged to address real-time performance needs and security threats in blockchain-based systems used for intrusion detection (Ramadan et al. 2021).

Our study now needs confirmation through experiments across different real-world environments like cities and weather extremes. Under Algorithmic optimization we need to create streamlined RL-based planning and HTS-AD software for smaller UAVs. Combining blockchain protection methods with alternative security structures such as federated learning reduces blockchain operational costs without sacrificing protection strength.

The article develops a strong framework using AI-powered drones to monitor network performance better than standard methods. The study lays out plans to develop scalable secure and functional UAV networks for future telecommunications systems while correcting the research's known weaknesses. The study proves that ongoing artificial intelligence and drone integration technology research will keep powering our future digital systems.

6. Conclusion

The study elucidates how AI-powered drones facilitate real-time network evaluations and address key telecommunications constraints, such as efficiency limitations and abnormal behavior detection. The findings demonstrate that UAV systems employing advanced AI algorithms enhance network surveillance by adapting to changes instantaneously. The system exhibits substantial network management benefits through the use of reinforcement learning for path optimization and hybrid detection algorithms that integrate temporal and spectral models.

The report highlights that UAV mission adaptability improves network performance across various locations and conserves resources. The integration of AI enhances network monitoring and enables the prediction of potential issues before they arise. UAVs are poised to play a significant role in future telecommunications systems, as their mobility allows companies to

meet the increasing demands from IoT, 5G, and emerging technology networks.

While the study presents promising results, it calls for further development in specific areas. Field tests are necessary to validate the system's performance under unexpected conditions. The research also necessitates improved resource optimization for operation on devices with limited power. Incorporating multiple security techniques into the system will mitigate new cyber threats while maintaining rapid response times.

The investigations pave the way for advancements in UAV network monitoring. Future research should focus on enhancing the framework by incorporating cooperative UAV drone groups, improving inter-drone communication, and testing the system for emergency response and remote infrastructure monitoring. These initiatives will ensure that AI-driven drones become a cornerstone of future network management technology.

The article introduces a pivotal method for integrating drone surveillance with artificial intelligence to enable immediate network performance monitoring. This advancement represents significant progress in enhancing system efficiency and coverage across broader areas and at higher speeds. The study's findings provide a valuable trajectory for technical development, outlining a pathway toward more effective drone-powered telecommunications networks operating at optimal performance levels.

References

Abbas, T. N. A., Hameed, R., Kadhim, A. A., and Qasim, N. H. (2024). Artificial intelligence and criminal liability: exploring the legal implications of ai-enabled crimes. *Encuentros. Revista de Ciencias Humanas, Teoría Social y Pensamiento Crítico.,* (22), 140-159. https://doi.org/:10.5281/zenodo.13386675

Ajakwe, S. O., Kim, D. S., and Lee, J. M. (2023). Drone Transportation System: Systematic Review of Security Dynamics for Smart Mobility. *IEEE Internet of Things Journal,* 10 (16), 14462-14482.https://doi.org/:10.1109/JIOT.2023.3266843

Aldaej, A., Ahanger, T. A., Atiquzzaman, M., Ullah, I., and Yousufudin, M. (2022). Smart Cybersecurity Framework for IoT-Empowered Drones: Machine Learning Perspective. *Sensors*, 22 (7). https://doi.org/:10.3390/s22072630.

Alsamhi, S. H., Almalki, F. A., Ma, O., Ansari, M. S., and Lee, B. (2023). Predictive Estimation of Optimal Signal Strength From Drones Over IoT Frameworks in Smart Cities. *IEEE Transactions on Mobile Computing,* 22 (1), 402-416. https://doi.org/:10.1109/TMC.2021.3074442

Alsamhi, S. H., Shvetsov, A. V., Kumar, S., Hassan, J., Alhartomi, M. A., Shvetsova,

S. V., Sahal, R., et al. (2022). Computing in the Sky: A Survey on Intelligent Ubiquitous Computing for UAV-Assisted 6G Networks and Industry 4.0/5.0. *Drones*, 6 (7). https://doi.org/:10.3390/drones6070177.

Cheng, N., Wu, S., Wang, X., Yin, Z., Li, C., Chen, W., and Chen, F. (2023). AI for UAV-Assisted IoT Applications: A Comprehensive Review. *IEEE Internet of Things Journal,* 10 (16), 14438-14461. https://doi.org/:10.1109/JIOT.2023.3268316

Dey, A., Islam, T., Phelps, C., and Kelly, C. (2023). Signal Processing Based Method for Real-Time Anomaly Detection in High-Performance Computing. 2023 IEEE 47th Annual Computers, Software, and Applications Conference (COMPSAC), 26-30 June 2023. https://doi.org/:10.1109/COMPSAC57700.2023.00037.

Do, H. T., Truong, L. H., Nguyen, M. T., Chien, C.-F., Tran, H. T., Hua, H. T., Nguyen, C. V., et al. (2021). Energy-Efficient Unmanned Aerial Vehicle (UAV) Surveillance Utilizing Artificial Intelligence (AI). *Wireless Communications and Mobile Computing,* 2021 (1), 8615367. https://doi.org/:10.1155/2021/8615367

Fu, R., Ren, X., Li, Y., Wu, Y., Sun, H., and Al-Absi, M. A. (2023). Machine-Learning-Based UAV-Assisted Agricultural Information Security Architecture and Intrusion Detection. *IEEE Internet of Things Journal,* 10 (21), 18589-18598. https://doi.org/:10.1109/JIOT.2023.3236322

Hashim, N., Mohsim, A., Rafeeq, R., and Pyliavskyi, V. (2019). New approach to the construction of multimedia test signals. *International Journal of Advanced Trends in Computer Science and Engineering,* 8 (6), 3423-3429. https://doi.org/:10.30534/ijatcse/2019/117862019

Hassija, V., Chamola, V., Agrawal, A., Goyal, A., Luong, N. C., Niyato, D., Yu, F. R., et al. (2021). Fast, Reliable, and Secure Drone Communication: A Comprehensive Survey. *IEEE Communications Surveys & Tutorials,* 23 (4), 2802-2832. https://doi.org/:10.1109/COMST.2021.3097916

Islam, A., and Shin, S. Y. (2023). A Digital Twin-Based Drone-Assisted Secure Data Aggregation Scheme with Federated Learning in Artificial Intelligence of Things. *IEEE Network,* 37 (2), 278-285. https://doi.org/:10.1109/MNET.001.2200484

Jawad, A. M., Qasim, N. H., and Pyliavskyi, V. (2022). Comparison of Metamerism Estimates in Video Paths using CAM's Models. 2022 IEEE 9th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T), 10-12 Oct. 2022. https://doi.org/:10.1109/PICST57299.2022.10238685.

Jing, Y., Qu, Y., Dong, C., Ren, W., Shen, Y., Wu, Q., and Guo, S. (2023). Exploiting UAV for Air–Ground Integrated Federated Learning: A Joint UAV Location and Resource Optimization Approach. *IEEE Transactions on Green Communications and Networking,* 7 (3), 1420-1433. https://doi.org/:10.1109/TGCN.2023.3242999

Khlaponin, Y., Izmailova, O., Krasovska, H., Krasovska, K., Bodnar, N., and Abbas, S. Q. (2024). Base of Models of the Information Security Risks Assessment System. 2024 35th Conference of Open Innovations Association (FRUCT). https://doi.org/:10.23919/FRUCT61870.2024.10516397.

Li, K., Ni, W., and Dressler, F. (2022). Continuous Maneuver Control and Data Capture Scheduling of Autonomous Drone in Wireless Sensor Networks. *IEEE*

Transactions on Mobile Computing, 21 (8), 2732-2744. https://doi.org/:10.1109/TMC.2021.3049178

Li, Z., Rios, A. L. G., and Trajković, L. (2021). Machine Learning for Detecting Anomalies and Intrusions in Communication Networks. *IEEE Journal on Selected Areas in Communications,* 39 (7), 2254-2264. https://doi.org/:10.1109/JSAC.2021.3078497

McEnroe, P., Wang, S., and Liyanage, M. (2022). A Survey on the Convergence of Edge Computing and AI for UAVs: Opportunities and Challenges. *IEEE Internet of Things Journal,* 9 (17), 15435-15459. https://doi.org/:10.1109/JIOT.2022.3176400

Qasim, N., and Fatah, O. (2022). The role of cyber security in military wars. *V International Scientific and Practical Conference: "Problems of cyber security of information and telecommunication systems" (PCSITS)". October 27 - 28, 2022, Kyiv, Ukraine*. https://www.researchgate.net/profile/Nameer-Qasim/publication/369899226_The_role_of_cyber_security_in_military_wars/links/6431beafad9b6d17dc44d44e/The-role-of-cyber-security-in-military-wars.pdf

Qasim, N., Pyliavskyi, V., and Solodka, V. (2019). Development of test materials for assessment broadcasting video path. *arXiv preprint arXiv:1907.11406*. https://doi.org/:10.48550/arXiv.1907.11406

Ramadan, R. A., Emara, A.-H., Al-Sarem, M., and Elhamahmy, M. (2021). Internet of Drones Intrusion Detection Using Deep Learning. *Electronics*, 10 (21). https://doi.org/:10.3390/electronics10212633.

Shakir, M. A., Abass, H. K., Jelwy, O. F., Al-Bayati, H. N. A., Salman, S. M., Mikhav, V., and Bodnar, N. (2024). Developing Interpretable Models for Complex Decision-Making. 2024 36th Conference of Open Innovations Association (FRUCT). https://doi.org/:10.23919/FRUCT64283.2024.10749922.

Shayea, I., Dushi, P., Banafaa, M., Rashid, R. A., Ali, S., Sarijari, M. A., Daradkeh, Y. I., et al. (2022). Handover Management for Drones in Future Mobile Networks—A Survey. *Sensors*, 22 (17). https://doi.org/:10.3390/s22176424.

Slimani, H., El Mhamdi, J., and Jilbab, A. (2024). Assessing the advancement of artificial intelligence and drones' integration in agriculture through a bibliometric study. *International Journal of Electrical and Computer Engineering (IJECE),* 14 (1), 878-890. https://doi.org/:10.11591/ijece.v14i1.pp878-890

Speth, S., Gonçalves, A., Rigault, B., Suzuki, S., Bouazizi, M., Matsuo, Y., and Prendinger, H. (2022). Deep learning with RGB and thermal images onboard a drone for monitoring operations. *Journal of Field Robotics,* 39 (6), 840-868. https://doi.org/:10.1002/rob.22082

Wang, J., Liu, Y., Niu, S., Jing, W., and Song, H. (2022). Throughput Optimization in Heterogeneous Swarms of Unmanned Aircraft Systems for Advanced Aerial Mobility. *IEEE Transactions on Intelligent Transportation Systems,* 23 (3), 2752-2761. https://doi.org/:10.1109/TITS.2021.3082512

Wang, L., Zhang, H., Guo, S., and Yuan, D. (2022). 3D UAV Deployment in Multi-UAV Networks With Statistical User Position Information. *IEEE Communications*

Letters, 26 (6), 1363-1367. https://doi.org/:10.1109/LCOMM.2022.3161382

Yang, Z., Chen, M., Liu, X., Liu, Y., Chen, Y., Cui, S., and Poor, H. V. (2021). AI-Driven UAV-NOMA-MEC in Next Generation Wireless Networks. *IEEE Wireless Communications,* 28 (5), 66-73. https://doi.org/:10.1109/MWC.121.2100058