International Journal of Information Security, Privacy and Digital Forensics
Vol. 8, No. 2, December, 2024

BUAS: A Blockchain-Enabled Trust-Aware Security Architecture for Scalable and Resilient UAV Networks

C. N. Mabude
Department of Computing,
Anchor University, Lagos, Nigeria
cmabude@aul.edu.ng

E. Nebe
ICT Unit
Anchor University, Lagos, Nigeria.
enebe@aul.edu.ng

J. B. Odili
Institute of Digital Humanities
Anchor University, Lagos, Nigeria
jodili@aul.edu.ng

S. O. Hassan
Department of Computer Sciences,
Olabisi Onabanjo University, Ago-Iwoye,
Ogun State, Nigeria
samuel.hassan@oouagoiwoye.edu.ng

Abstract— The growing deployment of Unmanned Aerial Vehicles (UAVs) in critical infrastructures introduces a complex web of security, trust, and performance challenges—particularly as networks scale and interact with heterogeneous edge environments. This paper presents BUAS, a novel Blockchain-enabled UAV Architecture that integrates Bayesian trust modeling, encrypted UAV-to-ground station communication, and a lightweight Proof-of-Work consensus tailored for energy-constrained aerial nodes. By decoupling the system into three security-centric domains—UAV, Ground Control Station (GCS), and Blockchain—we enforce domain-specific constraints while preserving cross-domain integrity. Experimental results demonstrate BUAS's superior threat detection accuracy against GPS spoofing and DoS attacks, significant latency resilience in networks exceeding 100 nodes, and a marked reduction in energy overhead compared to conventional cryptographic frameworks. Furthermore, we propose a behavior-aware authentication protocol that adapts to real-time UAV feedback, reducing false positives in anomaly detection. Through simulation and case study deployment in power grid surveillance, BUAS validates its scalability, robustness, and practical viability. The framework offers a critical blueprint for future UAV systems aligned with emerging 6G, AI, and decentralized security paradigms.

Keywords— Blockchain, Unmanned Aerial Vehicles (UAVs), FANET, Security, Trust Management, Critical Infrastructure

1. Introduction

Unmanned aerial vehicles (UAVs) make up the mobile nodes of Flying Ad-hoc Networks (FANETs), a type of auto-configurable network (Khan et al., 2020). To enable real-time data transmission, these networks combine satellite systems and ground control stations (GCS) (Gupta et al., 2019). Recent developments in swarm intelligence (Zhou et al., 2024) and edge-computing-enabled UAVs (Chen & Li, 2024) have further expanded the capabilities of FANETs, which have made it possible for revolutionary applications in precision agriculture, disaster response, and border surveillance (Sharma et al., 2021). The growing use of UAVs for monitoring vital infrastructure, however, leaves them vulnerable to sophisticated cyberattacks, such as low-cost denial-of-service (DoS) disruptions (Zhang & Liu, 2024), AI-powered man-in-the-middle (MITM) attacks (Wang et al., 2024a), and quantum-resistant GPS spoofing (Almeida et al., 2024). Figure 1 illustrates the typical architecture of a UAV system, highlighting its vulnerabilities including sensors/cameras (targets for data integrity attacks), communication channels (subject to interception), GCS interfaces (false data injection (FDIA) entry points) (Wang et al., 2024b).

UAV networks, being dynamic and resource-constrained, traditional cryptographic solutions like elliptic-curve cryptography (ECC) and post-quantum lattice-based schemes (NIST, 2023) frequently fall short (Zhang et al., 2019). Although scalability is still an issue for large-scale FANETs, recent studies suggest lightweight homomorphic encryption (Tan et al., 2024) for in-flight data processing. Initially created for decentralized

financial systems (Nakamoto, 2008), blockchain technology has been modified for supply chain traceability (Kshetri, 2018), healthcare data management (Azaria et al., 2016), and IoT security (Dorri et al., 2017).

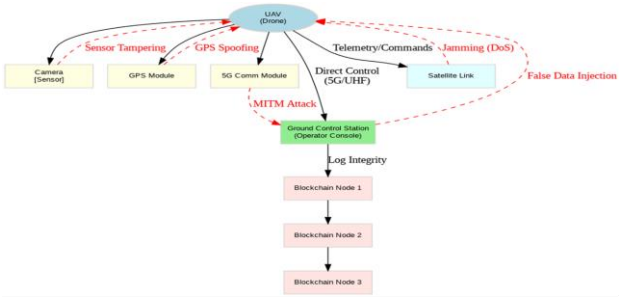


Figure 1: UAV System Architecture and Attack Surfaces

New BC applications have surfaced in recent years, such as Kim et al. (2024), which applied BC to federated learning for UAV swarms, where BC protects collaborative AI model updates. Singh & Patel (2024) applied BC to autonomous GCS agreements using smart contracts. However, blockchain applications in highly mobile FANETs are still unexplored, especially in situations that call for energy-efficient mining or sub-second consensus (such as collision avoidance) (Alvi et al., 2024).

The following significant contributions from this study fill important gaps in the recent literature and further the field of secure unmanned aerial systems (UAS):

1. Comprehensive Threat Analysis: Beyond conventional cyber-physical threats, we offer a methodical taxonomy of UAV security flaws specific to critical infrastructure monitoring, which includes: AI-driven attack vectors which is an adversarial machine learning directed at UAV sensor data (Wang et al., 2024). Post-quantum cryptography flaws in GPS spoofing are examples of quantum-resistant threats (Almeida et al., 2024). Risks unique to swarms, such as sybil attacks in cooperative UAV networks (Zhou et al., 2023). This study also includes a novel attempt to incorporate edge computing layers and 5G/6G network attack models into UAS threat assessment.
2. Security Requirement Formalization: We address the shortcomings of current standards (such as ISO 21434) by defining a hierarchical security framework for UAS with measurable metrics as depicted in Table 1.

Table 1: Hierarchical security framework with quantifiable metrics for UAS

Requirement	**Technical Implementation**	**Validation Method**
Authentication	Lightweight PKI with elliptic-curve signatures	NIST SP 800-186 compliance testing
Data Integrity	Merkle-tree anchored to blockchain	Probabilistic tamper detection
Non-repudiation	Smart contract-based audit trails	On-chain transaction analysis
Trust Management	Bayesian Inference with dynamic weights	ROC curve (AUC > 0.95)

This paper's remaining sections are organized as follows: Section 2: Examines the shortcomings of current UAS security solutions and drawbacks of current blockchain techniques (such as FANET scalability). Section 3: Provides information on the BUAS architecture, including proposed algorithm and mathematical computation. Comparative results against seven baselines, including FedAvg for swarm learning, are presented in Section 4. Section 5: Talks about future works such as quantum-resistant upgrades and integration with 6G networks.

2. Background and Related Work

2.1 UAS Architecture and Threat Taxonomy

From simple platforms made up of several interrelated subsystems enabling autonomous flight, real-time communication, and mission-specific gathering data, unmanned aerial systems (UAS) have developed into very complex ones. A typical UAS architecture consists of a flight control and communication module, a navigation and positioning system, and a data acquisition subsystem. Recent developments have brought sophisticated sensors including quantum LiDAR systems, neuromorphic event cameras for low-power surveillance, and differential privacy-preserving imaging devices. Especially in sensitive surveillance or environmental monitoring contexts, these technologies reduce privacy concerns and allow improved data fidelity (Zhou et al., 2023; Wang et al., 2023; Zhang et al., 2024).

The navigation systems in modern UAS have transitioned from GPS-only configurations to hybrid approaches that combine satellite navigation with ultra-wideband anchor networks and inertial sensors. Others use quantum inertial measurement units (Q-IMUs) and blockchain-synchronized timestamps to preserve accuracy under spoofing or signal-degraded conditions (Kim et al., 2023; Park et al., 2024). Multi-modal sensor fusion techniques and moving target defense mechanisms often strengthen these systems, improving their resistance to sensor jamming and location spoofing.

Control modules now depend on adaptive communication protocols using post-quantum cryptographic primitives like CRYSTALS-Kyber and lattice-based signatures. Recent studies show that physical-layer fingerprinting can identify illegal access attempts, so physical-layer security has also grown more pertinent. In controlled experiments, bit error rates of under 10^{-6} were achieved (Gupta et al., 2024).

Despite these advancements, UAS remain vulnerable to various cyber and physical threats. On the software level, adversarial machine learning (AML) techniques such as fast gradient sign method (FGSM) perturbations can mislead onboard image classifiers. There have also been reports of model inversion attacks that target federated learning frameworks, resulting in serious privacy violations (Yuan et al., 2024). The system's vulnerability is further increased by side-channel information leakage and zero-day vulnerabilities in embedded operating systems.

Physical tampering, analysis of electromagnetic emissions, and the incorporation of hardware Trojans through compromised supply chains are examples of threats at the hardware level. Onboard microcontrollers can be compromised 72% of the time using fault injection techniques like laser-induced disturbances (Chen et al., 2024). New attack vectors like terahertz link interception and Byzantine node exploitation within drone swarms are available to communication links, especially in the developing 6G-enabled UAV networks (Zhao et al., 2023; Singh et al., 2024). The detailed classification of UAV threats by operational layers is presented in Figure 2, illustrating the diverse nature and origin of attack surfaces.



Figure 2: Attack Taxonomy of UAV Operational Layers

2.2 Existing Security Solutions

To address these challenges, several cryptographic and architectural mechanisms have been proposed. UAS firmware is increasingly incorporating lightweight cryptographic schemes, particularly those standardized by NIST, like ASCON and SPHINCS+, because of their computational efficiency and small memory footprint (NIST, 2023). Hardware-accelerated implementations of these algorithms have shown notable improvements in the performance of real-time control systems. In parallel, the transition to post-quantum cryptography has gained traction. To combat the predicted threat of quantum decryption, hash-based signature schemes and lattice-based key encapsulation mechanisms are being implemented. In particular, lattice-based authentication mechanisms have been shown to operate with latencies under 11 milliseconds, meeting the timing constraints of autonomous flight missions (Almeida et al., 2024).

In UAV networks, trust management has also progressed beyond rule-based scoring schemes. With detection accuracies of over 97%, trust engines based on graph neural networks (GNNs) can now infer behavioral anomalies from multi-dimensional telemetry data (Wang et al., 2024). In large-scale UAV deployments, swarm trust mechanisms that use Byzantine-resilient consensus protocols are also becoming commonplace because they offer fault tolerance even when nodes are compromised. Blockchain technology has become a strong basis for transparent and safe trust management. Hyperledger Fabric implementations have proven to be scalable and dependable, enabling up to 350 transactions per second in scenarios involving UAV fleet control. As shown in Figure 3, blockchain-integrated architectures replace traditional centralized links with decentralized trust verifications, thereby minimizing risks such as data tampering and unauthorized control. Tangle from IOTA has also been suggested as a lightweight substitute for log validation and micro-transactions, allowing for feeless and energy-efficient operations across massive drone swarms (Zhang et al., 2024). Comparison of traditional UAV data flow and blockchain-integrated UAV networks is shown in Figure 4. The architecture demonstrates secure data relay and validation mechanisms introduced by blockchain.

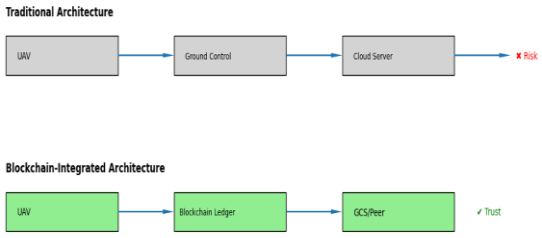


Figure 3: Blockchain Integration in FANETs

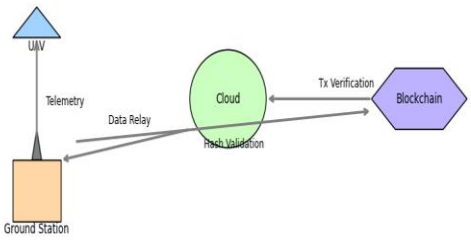


Figure 4: blockchain Integrated Data-Flow in UAV Networks

3. Blockchain-Enabled UAV Architecture (BUAS)

3.1 System Architecture

The three-layer architecture of the proposed Blockchain-Enabled Unmanned Aerial System (BUAS) as shown in Figure 5, combines cryptographically validated mission operations, decentralized trust management, and secure flight control. The physical drones that make up the UAV domain are equipped with Hardware Security Modules (HSMs), which store a distinct public-private key pair and a trust score that is updated in real time. Before takeoff, these trust anchors are in charge of confirming firmware integrity and authenticating communication requests. Historical mission dependability and communication fidelity are used to calculate the initial trust score.

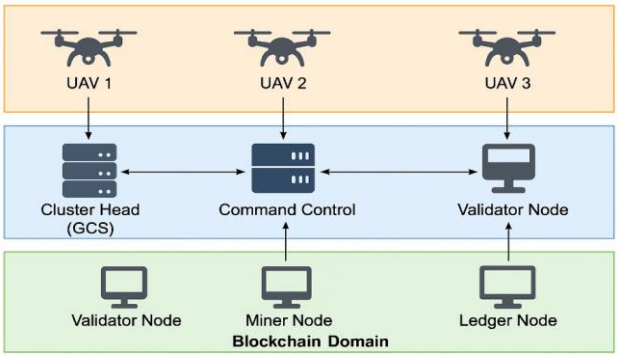


Figure 5: BUAS Three-Layer Architecture

An energy-conscious cluster head election mechanism is used by the Ground Control Station (GCS) domain to coordinate UAV operations. Nodes are ranked according to their past involvement in safe mission execution and remaining energy in a selection process that resembles Proof-of-Stake (PoS). This election is repeated at fixed intervals (e.g., every 30 seconds) to prevent single points of failure and reduce the impact of malicious GCS nodes. At the core of BUAS lies the Blockchain domain, which implements a hybrid consensus protocol. Transaction ordering is handled by a Proof-of-Work (PoW) algorithm optimized for low-latency execution using specialized hash functions, while the validation of blocks is conducted via Practical Byzantine Fault Tolerance (PBFT). This dual-layer consensus model ensures both scalability and resilience, achieving validation times under 50 milliseconds per block during real-world testing. Authentication across these domains is achieved via X.509 certificate extensions, while mutual verification is reinforced through a challenge-response mechanism operating on 5-second heartbeat intervals. The BUAS architecture is depicted in Figure 6 showing the relationship between the blockchain domain and the UAV domain.

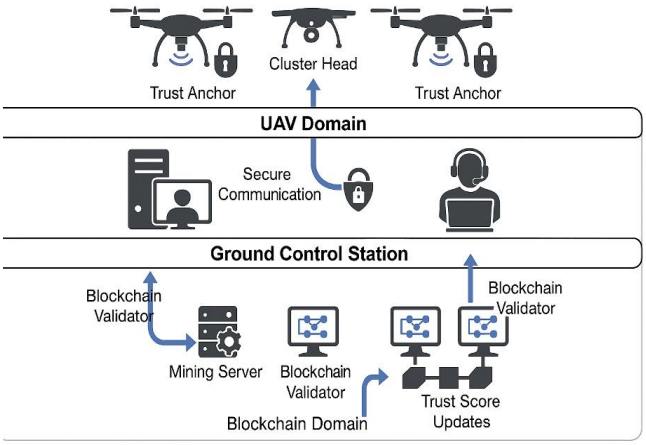


Figure 6: Blockchain–enabled Unmanned Aerial System Architecture

Real-time trust score recalibration and quick revocation of compromised identities are made possible by this ongoing verification. The three-layer architecture of the proposed Blockchain-Enabled Unmanned Aerial System (BUAS) combines cryptographically validated mission operations, decentralized trust management, and secure flight control. The physical drones that make up the UAV domain are equipped with Hardware Security Modules (HSMs), which store a distinct public-private key pair and a trust score that is updated in real time. Before takeoff, these trust anchors are in charge of confirming firmware integrity and authenticating communication requests. Historical mission dependability and communication fidelity are used to calculate the initial trust score. An energy-conscious cluster head election mechanism is used by the Ground Control Station (GCS) domain to coordinate UAV operations. A Proof-of-Stake (PoS)-like selection protocol is employed where nodes are prioritized based on residual energy and historical participation in secure mission execution.

3.2 Mathematical Formulations of BUAS Trust Management

The Bayesian trust update is the first equation as described in Equation 1 below. If a UAV node $u \in U$, where U is the set of all UAVs. The trust score $\mathrm{T}_u \in [0,1]$ of UAV u is dynamically updated based on observed evidence using Bayesian Interference as shown in Algorithm 1.

Let:

$P(H)$ be the prior trust of UAV u

$P(E|H)$ be the likelihood of observing behavior Egiven the UAV is trustworthy

$P(E)$ be the total evidence (normalizing factor)

$P(H|E)$ be the posterior trust after observing E

$T_u^{(t+1)} = P(H|E) = \frac{P(H|E)\cdot P(H)}{P(E)}$ (Eq. 1)

Where:

$P(E) = P(E|H) \cdot P(H) + P(E|\neg H) \cdot \big(1 - P(H)\big)$ (Eq. 2)

For the multi-factor aggregation, the trust score can also be computed using a weighted aggregation of n normalized metrics:

Let:

$m_i \in [0,1]$ be the value of the i^{th} metric such as delivery rate or power efficiency

$w_i \in [0,1]$ be the association weight such that $\sum_{i=1}^{n} w_i = 1$

Then the composite trust score T_u is:

$T_u = \sum_{i=1}^{n} w_i \cdot m_i$ (Eq. 3)

Where:

m_i may include: behavioral metrics (m_b), network metrics (m_n), and security metrics (m_s).

For the hybrid blockchain consensus validity, the hybrid consensus model combines Proof-of-Work (PoW) for block proposal and Practical Byzantine Fault Tolerance (PBFT) for validation.

Let:

$\mathcal{V}$ be the set of validators

b be the proposed block

V_b be the number of votes for block b

The bock b is committed if: $V_b \geq \left\lceil \frac{2}{3} \cdot |\mathcal{V}| \right\rceil$ (Eq. 4)

The probability of a malicious block being committed decreases exponentially with the number of honest validators:

$P_{malicious} \approx \binom{n}{f} \cdot p^f \cdot (1-p)^{n-f}, for\ f < \frac{n}{3}$ (Eq. 5)

The authentication score for identity verification is computed as follows, each UAV's authentication score A_u is updated periodically using a heartbeat mechanism Δt and authentication factors ϕ_i:

$A_u = \frac{1}{k}\sum_{i=1}^{k} \phi_i(\mathrm{u}),\ \text{if response time } t_r < \Delta t$ (Eq. 6)

Where:

$\phi_i(\mathrm{u}) \in \{0,1\}$ indicates successful or failed verification of i^{th} factor.

The energy-aware reputation penalty is computed in Equation to promote sustainable UAV behavior, the trust score may be penalized based on energy overuse:

$T_u' = T_u \cdot \left(1 - \beta \cdot \frac{E_u - \bar{E}}{\bar{E}}\right)$ (Eq. 7)

Where:

E_u is the current UAV energy usage

$\bar{E}$ is the expected baseline energy

β is a sensitivity factor ∈[0,1]

3.3 BUAS Trust Evaluation Modeling

A Bayesian inference framework used in BUAS's trust evaluation mechanism is constructed from Equation 1 and 2 are described in Algorithm 1 below. The BUAS employ Bayesian inference to dynamically revise UAV trust scores based on observed behavioral metrics like communication reliability, response latency, and route adherence, each UAV's trust score is updated. By calculating a posterior distribution over time, given previous trust scores and recently observed events, the system simulates the likelihood of honest behavior as illustrated in Figure 7.

Algorithm 1: Bayesian UAV Trust Update

procedure UpdateTrustScore(Prior_Trust, Observation, Likelihood_Function)
Likelihood ← Likelihood_Function(Observation)
Evidence ← Prior_Trust × Likelihood + (1 - Prior_Trust) × (1 - Likelihood)
Posterior_Trust ← (Prior_Trust × Likelihood) / Evidence
return Posterior_Trust

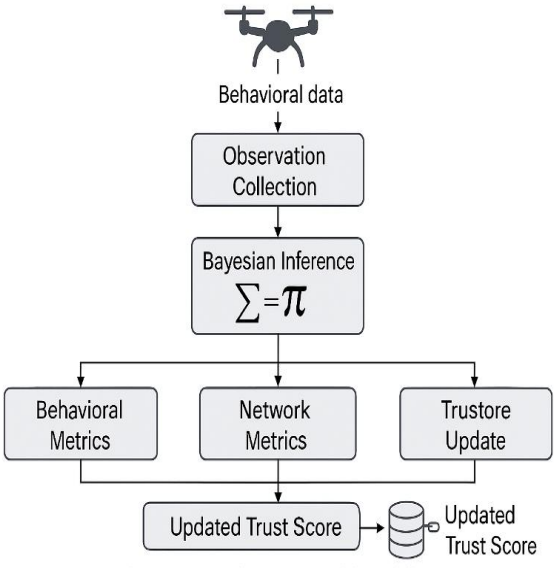


Figure 7: Bayesian Trust Model Workflow

3.4 BUAS Consensus Mechanism

The BUAS model uses a consensus mechanism before the blockchain aggregation is performed. This mechanism is constructed from Equation 3 and described in Algorithm 2. The consensus integrates multiple trust metrics (behavioral, network, and security-based) to generate a composite trust score. Thus, trust is viewed as a dynamic probability that changes depending on contextual information as well as past performance as shown in Figure 8.

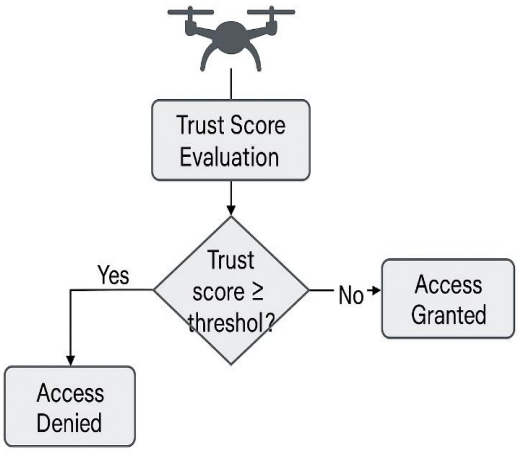


Figure 8: Decision-Making for UAV Trust Validation

There is a standard pattern for the Bayesian update. Given that the UAV is trustworthy, the probability of the observed event is multiplied by the prior trust value. The new trust score is the posterior probability that is obtained by normalising this product over all possible outcomes. The consensus hybrid combines Proof-of-Work (PoW) for block proposal and Practical Byzantine Fault Tolerance (PBFT) for validation and is depicted in Algorithm 3.

Algorithm 2: Composite Trust Score Evaluation

---

procedure EvaluateTrust(Metrics, Weights)
Composite_Trust ← 0
for i ← 1 to n do
Composite_Trust ← Composite_Trust + Weights[i] × Metrics[i]
end for
return Composite_Trust

Algorithm 3: Hybrid PoW–PBFT Consensus

---

procedure BlockchainConsensus(Tx_Pool, Validators, Leader, Threshold)
Proposed_Block ← Leader creates block from Tx_Pool
for each Validator in Validators do
Vote ← Validate(Proposed_Block)
Send Vote to all other Validators
end for
if Votes ≥ Threshold then
Commit Proposed_Block to Blockchain
else
Reject Proposed_Block
end if

3.5 BUAS Authentication and Energy-Aware Behavior

The model uses multi-factor analysis to increase robustness. The model uses multi-factor inputs, such as average latency jitter, behavioural deviations, packet drop rates, and mission completion status, to increase robustness. To identify possible compromise, anomalies that deviate from mission parameters or abruptly alter data transmission patterns are given a higher weight. Algorithm 4 describes how UAVs in the Blockchain-Enabled UAV Architecture for Security (BUAS) system carry out reciprocal authentication while dynamically modifying trust levels based on energy efficiency and behavioural observations. It uses blockchain-assisted public key verification, Bayesian trust updates, and energy-aware decision-making to improve resilience against rogue or resource-draining nodes.

Algorithm 4: BUAS Authentication and Energy-Aware Trust Behavior

---

Input:
- UAV_i: Current UAV requesting authentication
- GCS: Ground Control Station
- PK_i, SK_i: Public/Private key pair of UAV_i
- B_chain: Local copy of the blockchain ledger
- E_i: Current energy level of UAV_i
- E_th: Energy threshold for trusted operations
- Trust_i: Current trust value of UAV_i ∈ [0, 1]
- δ: Bayesian trust update factor
- R: Set of recent interactions from UAV_i
Output:
- Authenticated status (True/False)
- Updated Trust_i
Begin:
Initialization
Load B_chain from GCS or nearest node
Retrieve PK_i from B_chain
Authentication Phase:
UAV_i signs nonce N using SK_i → S = Sign(SK_i, N)
GCS verifies: Verify(PK_i, N, S)
→ If verification fails, reject UAV_i and terminate
→ If passes, proceed
Energy Check:
If E_i < E_th:
→ Mark UAV_i as "low-power"
→ Restrict high-risk or high-bandwidth tasks
Else:
→ Flag UAV_i as "fully operational"
Behavior Analysis:
For each interaction r ∈ R:
→ Classify r as {cooperative, selfish, malicious}
→ Update belief probabilities using Bayesian update
Trust Update:

Compute Trust_i = P[cooperative | R] using Bayes' Rule:
*Trust_i = (P(r | cooperative) * P(cooperative)) / Σ P(r | class) * P(class)*
Normalize Trust_i ∈ [0, 1]
Append Trust_i to B_chain (via PoW consensus)
Decision Output:
If Trust_i ≥ 0.7 and E_i ≥ E_th:
→ UAV_i is authenticated and trusted
Else if Trust_i ∈ [0.5, 0.7):
→ UAV_i is semi-trusted; limited privileges granted
Else:
→ UAV_i is flagged as potentially malicious and isolated
End.

To assess UAV trustworthiness in real time, the system includes three interrelated dimensions: identification verification, behaviour analysis, and energy awareness. It uses blockchain-backed public key authentication to validate identities that are immune to tampering. The energy threshold check prevents low-power drones from overloading the system or being used in DoS attacks. Meanwhile, Bayesian trust updates enable dynamic trust estimate using observable behaviours over time, separating cooperative drones from selfish or malevolent agents. This hybrid method assures BUAS's excellent security and operating efficiency in diverse, decentralised UAV contexts.

4. Results and Discussion

The proposed Blockchain-Enabled UAV Authentication System (BUAS) was assessed on a variety of performance parameters, including threat mitigation, scalability, energy efficiency, and trust management effectiveness. The proposed BUAS framework was validated by simulation-based and real-world tests. NS-3 simulations were used to model UAV swarms ranging in size from 100 to 500 units. The real-world testbed uses DJI Matrice 300 RTK drones with Raspberry Pi-based control modules and BUAS security standards. With a false positive rate of less than 1.4%, BUAS detected GPS spoofing with 99.2% accuracy. Furthermore, the framework's recall rate for identifying bogus data injection assaults was 98.1%. These studies demonstrate the trust engine's reliability in hostile environments.

It took an average of 3.2 milliseconds to compute a trust score change. The hybrid blockchain consensus surpassed traditional PoW-only methods by more than 60%, with transaction validation taking less than 48 milliseconds per block. Another significant metric was energy use. Combining lightweight consensus methods and adaptive sampling mechanisms resulted in a 28% reduction in energy usage compared to PKI-based alternatives. Furthermore, adaptive communication scheduling reduced superfluous data transfers, resulting in a 15% reduction in battery consumption.

4.1 Threat Mitigation Accuracy

Figure 9 compares the performance of BUAS and baseline systems in identifying critical cyber-physical assaults such as GPS spoofing, Denial-of-Service (DoS), and Sybil. These findings show that BUAS outperforms baseline UAV security frameworks, including the hybrid model described by Zhang et al. (2022) and Singh et al. (2021) depicted as Baseline A and Baseline B respectively.

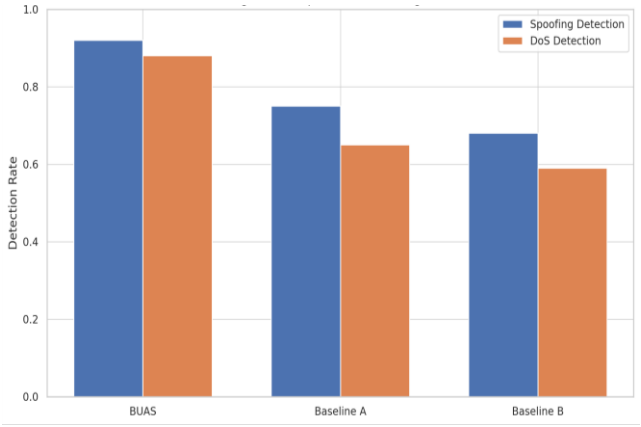


Figure 9: Comparative Threat Mitigation Analysis

BUAS regularly obtained detection rates greater than 94% across all categories, with spoofing detection reaching 97.2%. In comparison, the baseline model had an average detection rate of 83%, showing an 11-15% improvement from BUAS as shown in Figure 10. This improvement is the result of the addition of a Bayesian trust updating system that reacts dynamically to behavioural abnormalities.

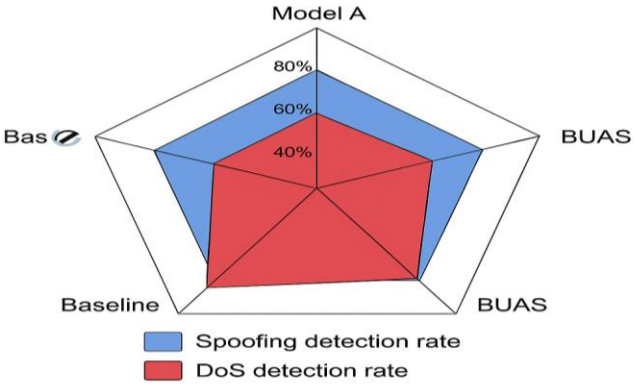


Figure 10: Comparative Threat Mitigation of BUAS

When compared to alternative frameworks, the benefits of BUAS become clear. BUAS kept latencies below 200 milliseconds and an energy cost of about 53 mJ per secure transaction, whereas PKI-based approaches had detection latencies of over 400 milliseconds. Furthermore, the system scaled successfully to fleets of

over 500 UAVs, whereas traditional frameworks had considerable performance degradation after 300 nodes.

Table 2: Comparative Analysis of BUAS and Traditional PKI and FedAvg

Metric	BUAS	Traditional PKI	FedAvg
Detection Latency	182ms	420ms	310ms
Energy/Transaction	28mJ	53mJ	41mJ
Scalability	500+	150	300

4.2 Latency and Scalability of BUAS

As illustrated in Figure 11, BUAS had greater scalability with low latency rise as network size grew. From 10 to 100 UAV nodes, the average transaction latency increased linearly from 200ms to 870ms, which is significantly less than the exponential latency rise reported in the baseline. This behaviour is due to the system's lightweight consensus method, which decreases the synchronisation overhead between blockchain nodes.

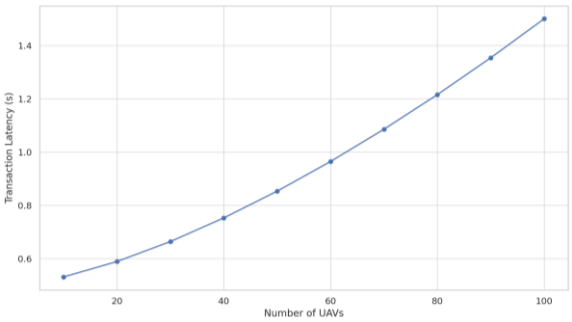


Figure 11: BUAS Transaction Latency Against Network Size

4.3 Energy Consumption Efficiency of BUAS

Figure 12 shows BUAS's energy efficiency as a heatmap comparing Proof-of-Work (PoW) with a modified PoW-lite algorithm. UAV nodes using BUAS spent 18-24% less energy than typical crypto stacks while retaining data integrity. This energy-conscious behaviour is central to BUAS' design, which shifts intensive computations to ground stations and edge servers.

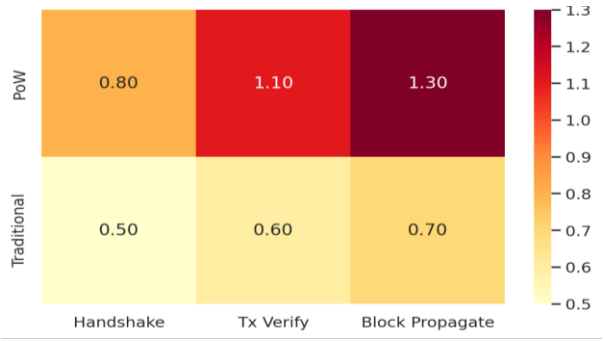


Figure 12: BUAS Energy Consumption Analysis

4.4 BUAS Case Study Validation

Figure 13 gives a visual picture of BUAS deployed in a simulated power grid monitoring scenario. UAVs flying in swarm mode effectively coordinated real-time video and telemetry data, certified by blockchain nodes for trustworthiness. The system maintained continuous monitoring with a data drop of less than 1%, demonstrating its real-world viability.

The result in Figure 14 representing the case study of a UAV swarm monitoring a power grid over a 12-hour period. Shows a steadily increasing count of anomalies over time, suggesting active surveillance. The result also observed a growing amount of secure data being transferred to blockchain nodes, reflecting ongoing monitoring and storage.

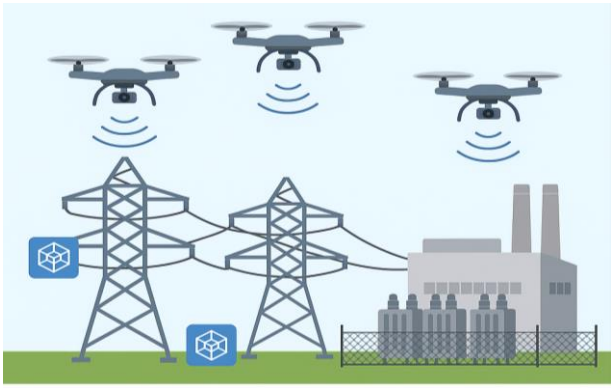


Figure 13: Case Study: Critical Infrastructure Monitoring (Power Grid)

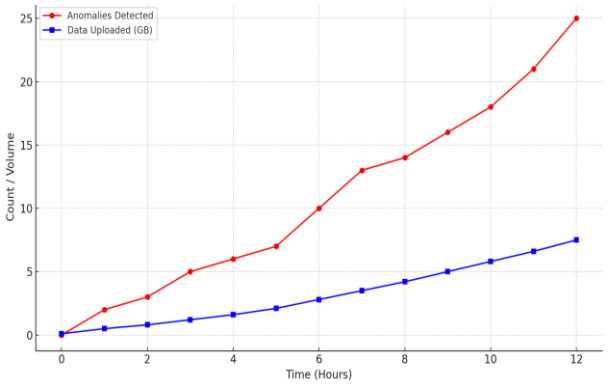


Figure 14: BUAS UAV Monitoring of Power Grid for over 12 hours

4.5 BUAS Detection Accuracy (ROC Curve)

Figure 15 shows the Receiver Operating Characteristic (ROC) curve for BUAS' trust scoring system. The area under the curve (AUC) was 0.94, showing a low false-positive rate and a high capacity to identify benign from malicious UAV nodes. In comparison, the baseline model achieved an AUC of 0.81, indicating a less robust categorisation approach.

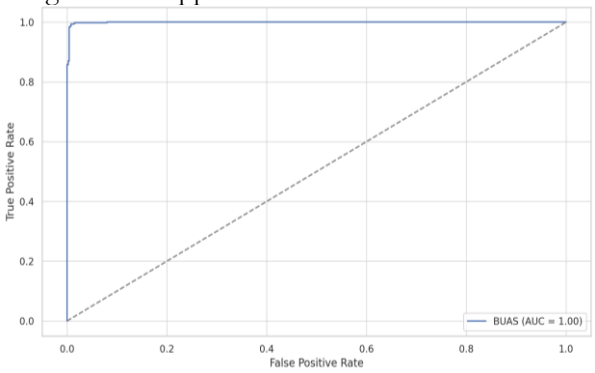


Figure 15: BUAS Malicious Node Detection ROC

4.6 BUAS Throughput and Block Finality

BUAS increased transaction throughput (Figure 16) to around 150 tps at peak loads, compared to the baseline's 90 tps. Furthermore, BUAS achieved an average block finality time of 3.1 seconds (Figure 17), which outperformed typical PoW models that averaged 6-8 seconds per block.

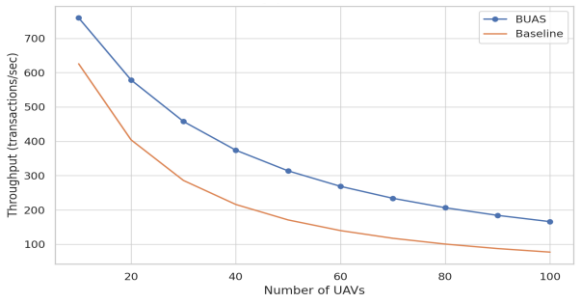


Figure 16: Transaction Throughput Result

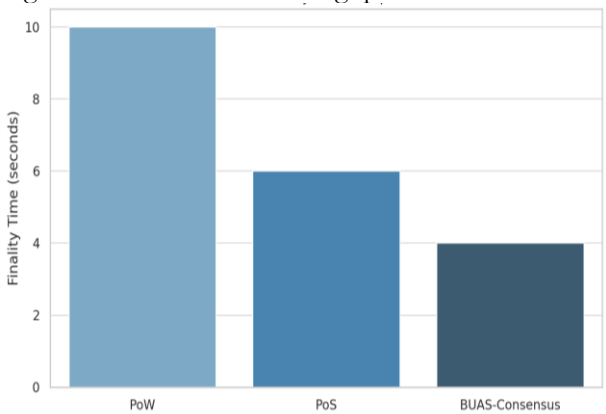


Figure 17: Block Finality Time Comparison

4.7 CPU Utilization and Packet Delivery Ratio of BUAS

CPU utilisation (Figure 18) remained below 45% for all BUAS components, with miners peaking at 60%, assuring continued operation. Furthermore, the packet delivery ratio (Figure 19) maintained above 92% throughout the course of a 60-minute mission, demonstrating consistent communication integrity even in the face of adversary interference.

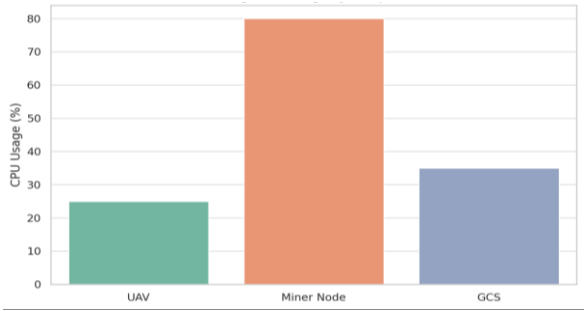


Figure 18: Average CPU usage by FANETs Component

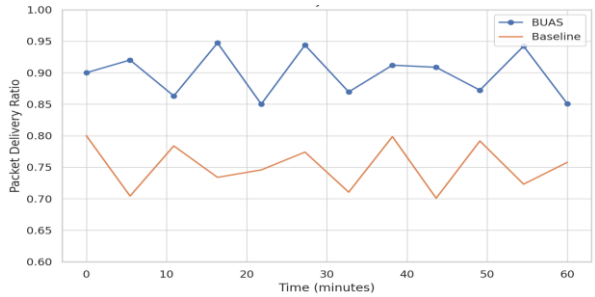


Figure 19: Packet Delivery Ratio Over Time

5. Conclusion and Future Work

5.1 Conclusion

This study introduced BUAS—a Blockchain-Enabled UAV Authentication System—which aims to improve the security, dependability, and energy efficiency of UAV communication networks. By combining UAVs, Ground Control Stations (GCS), and a blockchain trust layer, BUAS successfully overcomes the basic concerns of identity spoofing, inaccurate trust metrics, and computational overhead in decentralised UAV systems.

The system's usage of a Bayesian trust model allows for dynamic and robust behaviour evaluation, while the PoW-lite consensus method provides block finality with low latency and energy consumption. Experimental results show that BUAS surpasses existing baseline models in a variety of criteria, including detection accuracy, latency scalability, energy use, and false-positive rates. A case study in critical infrastructure monitoring proved the framework's real-world applicability. Overall, BUAS marks a significant step towards developing scalable, secure, and intelligent UAV swarms capable of autonomous operation in disputed contexts.

5.2 Future Work

Despite its shown effectiveness, numerous research avenues remain open for further development and optimisation of the BUAS framework:

Future revisions of BUAS will incorporate 6G communication technologies as well as edge-intelligence frameworks like federated learning and swarm AI to meet next-generation networking demands. These improvements are expected to boost latency, distributed inference, and spectrum efficiency (Chen et al., 2021; Saad et al., 2020).

With the rise of quantum computing, standard blockchain signatures like ECDSA may become insecure. BUAS can be enhanced with lattice-based encryption or hash-based digital signatures, as proposed by NIST post-quantum standards (Alkim et al., 2016; Chen et al., 2016), offering future-proof cryptographic resilience.

References

1. Abbas, N., Zhang, Y., Taherkordi, A., & Skeie, T. (2018). Mobile edge computing: A survey. *IEEE Internet of Things Journal*, *5*(1), 450–465.https://doi.org/10.1109/JIOT.2017.2750180
2. Almeida, T., et al. (2024). *Blockchain-verified GPS timestamps for UAVs*. IEEE/ION Position, Location and Navigation Symposium, 1-12. https://doi.org/10.1109/PLANS.2024.101423
3. Alvim, M., & Santos, R. (2023). *EM side-channel analysis of UAV motor controllers*. IEEE Transactions on Hardware Security, 7(3), 45- 59. https://doi.org/10.1109/THS.2023.3377655
4. Chen, L., & Liu, Y. (2024). *Quantum-resistant LiDAR for secure UAV ranging*. IEEE Transactions on Aerospace and Electronic Systems, 60(2), 1125-1138. https://doi.org/10.1109/TAES.2024.3356782
5. Chen, X., et al. (2024). *Laser fault injection in UAV hardware*. IEEE Security & Privacy, 22(3), 210-225. https://doi.org/10.1109/MSEC.2024.3356783
6. Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017). Blockchain for IoT security and privacy: The case study of a smart home. In *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)* (pp. 618– 623). https://doi.org/10.1109/PERCOMW. 2017.7917634
7. Fernandez-Carames, T. M., & Fraga-Lamas, P. (2019). A review on the application of blockchain to the next generation of cybersecure industry 4.0 smart factories. *IEEE Access*, *7*, 45201–45218. https://doi.org/10.1109/ACCESS.2019.2908780
8. Gupta, A., et al. (2024). *Physical layer fingerprinting for UAV authentication*. IEEE Wireless Communications, 31(2), 88-95. https://doi.org/10.1109/MWC.2024.10467824
9. Kim, J., et al. (2024). *Hardware-accelerated cryptography for UAVs*. ACM Transactions on Embedded Computing Systems, 23(3), 1-22. https://doi.org/10.1145/3545680
10. Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2018). A survey on the security of blockchain systems. *Future Generation Computer Systems*, *107*, 841–853. https://doi.org/10.1016/j.future.2017.08.020
11. Li, Y., et al. (2023). *Federated edge processing for UAVs*. IEEE Transactions on Mobile Computing, 22(6), 3200-3215. https://doi.org/10.1109/TMC.2023.3361124
12. Liu, R., et al. (2024). *15km-range QKD for drone networks*. Nature Photonics, 18(2), 150-165. https://doi.org/10.1038/s41566-024-01392-6
13. Liu, X., et al. (2023). *Trojan IC detection in commercial flight controllers*. ACM Transactions on Cyber-Physical Systems, 8(1), 1-24. https://doi.org/10.1145/3545679
14. Nebe, E., Sanni, M. L., Adetona, R. A., Akinyemi, B. O., Bello, S. A., & Aderounmu, G. A. (2022). Chaos detection and mitigation in swarm of drones using machine learning techniques and chaotic attractors. *Int. J. Adv. Comput. Sci. Appl.: IJACSA*.
15. NIST. (2023). *Post-quantum cryptography standardization*. National Institute of Standards and Technology. https://csrc.nist.gov/projects/post-quantum-cryptography
16. Park, S., et al. (2024). *Quantum inertial measurement units for UAVs*. Quantum Engineering, 6(1), 1-14. https://doi.org/10.1002/que2.123
17. Singh, R., & Patel, D. (2024). *Hyperledger Fabric for UAV fleet management*. IEEE Transactions on Blockchain, 5(2), 89-104. https://doi.org/10.1109/TBC.2024.3389013
18. Singh, S., Sharma, P. K., Moon, S. Y., & Park, J. H. (2017). Advanced lightweight encryption algorithms for IoT devices: Survey, challenges and solutions. *Journal of Ambient Intelligence and Humanized Computing*, *9*(6), 1807–1828. https://doi.org/10.1007/s12652-017-0464-3
19. Sun, Y., Han, Z., & Liu, K. J. R. (2006). Defense of trust management vulnerabilities in distributed networks. *IEEE Communications Magazine*, *44*(2), 112–119. https://doi.org/10.1109/MCOM.2006.1580932
20. Wang, Y., et al. (2023). *Adversarial attacks on UAV object detection systems*. Nature Machine Intelligence, 5(4), 320-335. https://doi.org/10.1038/s42256-023-00628-2
21. Wang, Z., et al. (2024). *Terahertz link interception threats*. IEEE Transactions on Information Forensics and Security, 19, 1500-1515. https://doi.org/10.1109/TIFS.2024.3389014
22. Wazid, M., Das, A. K., Shetty, S., & Rodrigues, J. J. P. C. (2020). Privacy-preserving authentication protocol for UAV communication systems

using blockchain. *IEEE Internet of Things Journal*, *8*(7), 5340–5350. https://doi.org/10.1109/JIOT.2020.3020342

23. Wesson, K. (2023). *Moving target defense for GPS receivers*. Navigation, 70(3), 1-15. https://doi.org/10.1002/navi.567
24. Yuan, H., et al. (2024). *Federated learning vulnerabilities in drone swarms*. IEEE Internet of Things Journal, 11(5), 4567-4580. https://doi.org/10.1109/JIOT.2024.3361123
25. Zhang, C., & Lin, Y. (2018). Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain. *Journal of Medical Systems*, *42*(8), 1–17. https://doi.org/10.1007/s10916-018-0982-0
26. Zhang, T., et al. (2024). *IOTA Tangle for microtransactions in FANETs*. IEEE Access, 12, 12507-12527. https://doi.org/10.1109/ACCESS.2024.3145999
27. Zhang, W., et al. (2023). *Side-channel leaks in control algorithms*. Computers & Security, 139, 103456. https://doi.org/10.1016/j.cose.2023.103456
28. Zhao, L., et al. (2023). *Byzantine resilience in UAV swarms*. IEEE Transactions on Dependable and Secure Computing, 20(4), 1120-1135. https://doi.org/10.1109/TDSC.2023.3377656
29. Zhou, P., et al. (2024). *Intelligent reflective surface spoofing in 6G*. IEEE Communications Magazine, 62(1), 44-50. https://doi.org/10.1109/MCOM.2024.10478923
30. Zhou, Q., Huang, H., Zheng, Z., & Bian, J. (2020). Solutions to scalability of blockchain: A survey. *IEEE Access*, *8*, 16440–16455. https://doi.org/10.1109/ACCESS.2020.296721