SABEC: Secure and Adaptive Blockchain-Enabled Coordination Protocol for Unmanned Aerial Vehicles(UAVs) Network

Hulya Dogan[a] and Anton Setzer[b]
Department of Computer Science, Swansea University, Swansea, U.K.

Keywords: UAVs Network, Byzantine Attack, Swarm Drone, Blockchain, Security, Proof of Work (PoW), Fuzzy C-Modes Clustering Algorithm, Fault Tolerance.

Abstract: The rapid advancement of drone swarm technology has unlocked a multitude of applications across diverse industrial sectors, including surveillance, delivery services, disaster management, and environmental monitoring. Despite these promising prospects, ensuring secure and efficient communication and coordination among drones within a swarm remains a significant challenge. Key obstacles include maintaining efficiency, facilitating the seamless sharing of sensing data, and achieving robust consensus in the presence of Byzantine drones—malicious or faulty *UAV*s capable of disrupting swarm operations and leading to catastrophic outcomes. To address these challenges, we introduce *SABEC* (Secure and Adaptive Blockchain-Enabled Coordination Protocol), an innovative blockchain-based approach designed to manage multi-drone collaboration during swarm operations. *SABEC* improves the security of the consensus achievement process by integrating an efficient blockchain into the *UAV* network, coupled with a practical and dynamic consensus mechanism. The protocol incentivizes network devices through a scoring system, requiring *UAV*s to solve intricate problems employing the Proof of Work (*PoW*) with Fuzzy C-Modes clustering algorithm. Leader *UAV*s are dynamically selected within clusters based on a predefined threshold, tasked with transmitting status control information about neighbouring *UAV*s to a cloud server. The server consolidates these data through a robust consensus mechanism, relaying them to the network coordination tier where decision-making consensus is reached, and the data are immutably stored on the blockchain. To facilitate the dynamic and adaptive construction of configurable trusted networks, *SABEC* employs a consensus protocol based on the blockchain-assisted storage. Comparative experiments conducted using *NS3* simulation software demonstrate *SABEC*'s significant advantages over traditional routing and consensus protocols in terms of packet delivery rate, coordination overhead, and average end-to-end delay. These improvements collectively enhance the fault tolerance of *UAV* networks, ensuring high availability and reliability even in the presence of adversarial nodes. By augmenting the security of consensus achievement, *SABEC* substantially improves connectivity, security and efficiency within intelligent systems, thereby elevating the potential and stability of multi-drone applications in real-world scenarios.

1 INTRODUCTION

In the era of 4.0 industry, the widespread integration of autonomous robotic systems has revolutionized various sectors, such as healthcare (F. Cunico et al., 2024), self-driving automobiles (Asilian et al., 2023), smart manufacturing (Yucesoy et al., 2024), and agriculture (Tang et al., 2024). This paradigm shift in robotics research has transitioned from developing and operating sophisticated single-robot systems to exploring multi-robot or swarm-robot systems. The ability to integrate simple individual robot actions into collaborative missions involving multiple robots has enabled the accomplishment of higher-level tasks through interaction and collaboration within vast robotic systems. Despite individual robots being relatively uncomplicated and limited in capability, they can exhibit sophisticated collective behaviours at the multi-robot level (Pajany et al., 2024). Notably, drones have emerged as pivotal aerospace robots, facilitating diverse real-world applications. The advent of smart manufacturing and smart cities has

[a] https://orcid.org/0009-0000-1841-2968
[b] https://orcid.org/0000-0001-5322-6060

Dogan, H. and Setzer, A.
SABEC: Secure and Adaptive Blockchain-Enabled Coordination Protocol for Unmanned Aerial Vehicles(UAVs) Network.
DOI: 10.5220/0013330500003899

In *Proceedings of the 11th International Conference on Information Systems Security and Privacy (ICISSP 2025) - Volume 1*, pages 377-388
ISBN: 978-989-758-735-1; ISSN: 2184-4356

underscored the increasing importance of real-time, efficient, and secure environment monitoring systems, which rely on Unmanned Arial Vehicles (*UAVs*) for enhanced functionality (Chung et al., 2018). *UAV* enables collaboration among drones and their access to restricted airspace, thereby bolstering air traffic management (Jin et al., 2003), logistics monitoring (Queralta et al., 2020), smart mobility (Yang et al., 2024), public safety (Lou et al., 2024), and environmental applications (Du et al., 2024). Drones have found extensive utility in numerous domains, including package delivery (Dogan et al., 2023), environmental monitoring (Wang et al., 2024), collaborative operations with other robot types in smart manufacturing (Silva et al., 2024), traffic monitoring in smart cities (Amarcha et al., 2024), and public safety and disaster management. These applications share a common requirement of navigation and airspace control (Salim et al., 2024). Moreover, large-scale environmental monitoring necessitates the coordination of a group of drones due to individual drones' limited mobility and capabilities. Consequently, coordinated control strategies and practical consensus algorithms are indispensable to ensure *UAV* systems' stability, safety, energy efficiency, and trustworthiness. However, the inherent heterogeneity and complexity of *UAV* systems necessitate the development of efficient and adaptable network designs to ensure proper functioning and safety. Blockchain technology, specifically consensus algorithms, offers a decentralized and scalable solution for achieving consensus among multi-drones while enhancing security and trustworthiness in *UAV* networks (Chen et al., 2024; Alsamhi et al., 2022; Jin et al., 2024). Integrating blockchain into multi-drone systems has emerged as a prominent research area, providing solutions for controlling Byzantine drones and addressing the consensus problem. Furthermore, specific aspects of collaboration requiring the sharing of sensitive data among drones can be secured by incorporating elements of the blockchain stack, such as the Merkle Tree technique (Jiang et al., 2020). Consequently, multi-drone systems necessitate consensus among drones to enable real-time, collaborative, and efficient task execution. Subsequent investigations since 2018 have explored various blockchain applications in the swarm of *UAV*s, encompassing consensus achievement of swarms in the presence of Byzantine drones, management of collaboration in heterogeneous *UAV* systems, and secure data collection. Nonetheless, this study investigates the utilization of blockchain technology to manage drone collaboration in a multi-drone system, emphasizing the sharing of sensor data capability, which poses a significant challenge in multi-drone collaboration. Considering that drones exhibit varying numbers, types, and data analysis rates, it is crucial to establish an automatic consensus mechanism for drones. The objectives of applying consensus algorithms in blockchain systems align with those of swarm design. Firstly, blockchain functions as a distributed decision-making system that operates without the need for trust between participating entities, mirroring the operating conditions of swarms (Liang et al., 2024). Secondly, since blockchain systems incorporate procedures to maintain information integrity, swarms established through these procedures do not require additional nodes for verifying operational records (Khan et al., 2024). Thirdly, the loss of a single drone, akin to the loss of an individual node in any decentralized system, should maintain the consensus-reaching process (Jiang et al., 2024). Proof of Work (*PoW*), a decentralized consensus technique, compels network participants to invest time in solving arbitrary mathematical puzzles to prevent malicious influences (Sedjelmaci et al., 2017). In this study, we implemented a new practical and dynamic protocol using *PoW* consensus to generate the difficulty factor in the *UAV* network and the dynamic clustering selection frequency. This approach provides drones with enhanced accuracy, usability and mitigates the risk of malicious attackers/ Byzantine drones sharing tampered data.

UAV networks possess qualities such as affordability, easy and flexible deployment, and high resistance to destruction, making them extensively utilized in numerous fields (Bertrand et al., 2024). In recent years, the domestic consumer-grade *UAV* market has reached saturation, leading to the prominence of industrial-grade *UAV*s in the emerging industry. Collaborating with traditional sectors, *UAV* networks have become indispensable aerial platforms, playing irreplaceable and crucial roles in various specialized environments, including security monitoring, emergency disaster mitigation, rescue operations, exploration, and digital cities (Kundu et al., 2024). Despite progress in swarm drone technology, drones remain vulnerable to jamming, trapping (Fang et al., 2022), and attacks (Hughes et al., 2024) due to their limited resources, the open nature of wireless communications, and the need for more aerial countermeasures (Li et al., 2021). Mission-oriented *UAV* networks operate in highly dynamic, complex, and unstructured environments where network size, topology, and node trustworthiness constantly change. Enhancing network fault tolerance and maintaining trustworthiness during missions pose significant challenges for distributed *UAV* networks, given their limited resources and lack of central support (He et al., 2020). *UAV* networks operating in mission-oriented environments face three significant unfavourable conditions: non-security, complex operation environments, lack of central support, and limited resources of network nodes. Thus, enhancing fault tolerance and maintaining trustworthiness during missions pose major challenges for distributed *UAV* networks with limited resources and no central support. Mission-oriented *UAV* networks operate in highly dynamic, complex, and unstructured environments where network size, topology, and trustworthiness of network nodes continuously change. Consequently, unauthorized access by external nodes must be prevented along with tolerating internal error nodes that may emerge within *UAV* nodes due to consumption, damage, or compromise.

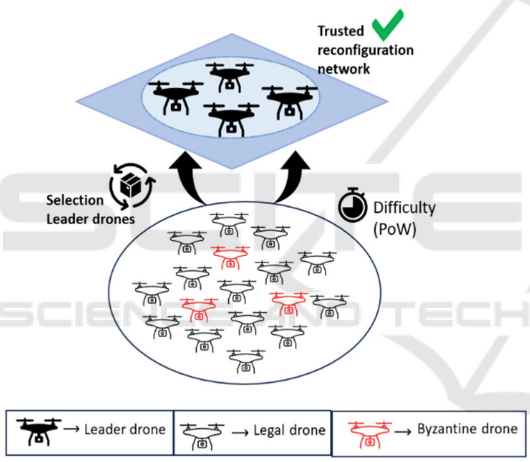

Figure 1: Network Architecture of the System.

2 CONTRIBUTIONS

This paper introduces the Secure and Adaptive Blockchain-Enabled Coordination (*SABEC*) protocol, which addresses the dynamic nature of *UAV* networks by leveraging blockchain technology combined with the Proof-of-Work (*PoW*) mechanism (Abishu et al., 2024) and Fuzzy C-Means Clustering (FCM) algorithm (Sun et al., 2024). SABEC ensures secure network participation and leader election through rigorous verification processes, enhancing protection against Byzantine drones and other security threats. Leader drones, validated through PoW, are responsible for securely transmitting data to a base station server, which aggregates and evaluates data, storing results on a blockchain for integrity and reliability. The adaptive consensus mechanism introduced by *SABEC* efficiently handles network topology changes and node reliability by recording health assessments and facilitating automatic reconfiguration of the network. The clustering algorithm within *SABEC* periodically selects cluster heads based on trust metrics, forming an upper-layer network to manage operations. This dynamic clustering approach optimizes resource usage, enhances fault tolerance, and supports efficient collaboration among *UAV*s. *SABEC* provides an innovative solution for secure *UAV*s network, adaptive leader election, efficient consensus, and reliable data storage, significantly advancing *UAV* network coordination by improving trust, scalability, and resilience.

3 NETWORK ARCHITECTURE

This The network architecture of the Secure and Adaptive Blockchain-Enabled Coordination Protocol (*SABEC*) is presented, an innovative cross-layer protocol designed to optimize *UAV* network performance through adaptive trust management and blockchain technology. *SABEC* addresses critical challenges such as excessive coordination overhead, dynamic node density, and Byzantine faults, thereby ensuring high network availability and trustworthiness. By leveraging advanced blockchain technology and innovative consensus algorithms, *SABEC* provides a scalable and secure framework adaptable to the dynamic and resource-constrained environments in which *UAV* networks operate. The architecture of *SABEC* is meticulously designed to operate across multiple network tiers, facilitating seamless information exchange and task collaboration among *UAV* nodes. The protocol integrates blockchain technology to enhance security and trust management, ensuring that only reliable nodes participate in the network's upper management layer. The architecture is compartmentalized into distinct tiers, each responsible for specific functionalities essential to the framework's performance and reliability.

Signal Transmission and Access Coordination Tiers: At the foundational signal transmission tier, the Proximal Node Discovery and Monitoring Component protocol (*PDMC*) is responsible for the accurate detection and continuous monitoring of adjacent *UAV* nodes. *PDMC* employs enhanced signal processing techniques to identify neighbouring nodes reliably, even in environments with high

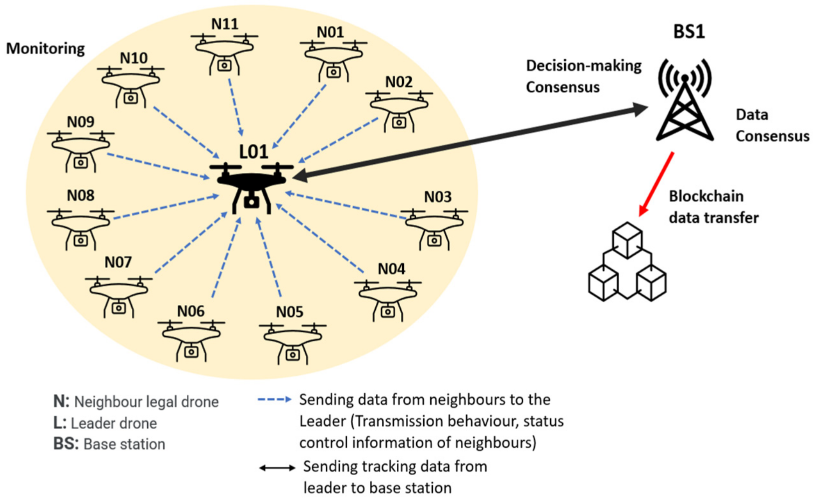

Figure 2: Blockchain-Enhanced for Swarms of drone network Architecture.

interference and node mobility. This component protocol establishes a dependable foundation for subsequent routing decisions by maintaining up-to-date neighbour tables and monitoring the forwarding behaviours of adjacent nodes.

Data Coordination Tiers: The data coordination tier integrates three pivotal component protocols that collectively manage local network and cross-network communications: ***Localized Trust Coordination Component protocol (LTCC):*** This component protocol manages local zone communications by evaluating and prioritizing coordination paths through trusted nodes based on real-time assessments. LTCC minimizes internal zone coordination overhead by selecting optimal paths that reduce latency and enhance data delivery efficiency. ***Hierarchical Trust-Based Coordination Component protocol (HTCC):*** Facilitating external communications, HTCC establishes hierarchical coordination paths that connect different network zones through trusted gateway nodes. HTCC employs dynamic clustering algorithms to form and manage hierarchical structures, thereby enhancing scalability and reducing coordination complexity. ***Secure Border Coordination Component protocol (SBCC):*** Overseeing data transmission across network boundaries, SBCC ensures secure and efficient coordination between zones. SBCC integrates blockchain-based verification mechanisms to authenticate coordination information and prevent the dissemination of malicious data.

Service Management and Control Tiers: At the pinnacle of the architecture, the service management tier incorporates the Secure and Adaptive Blockchain-Enabled Coordination Protocol (*SABEC*). *SABEC* serves as the core component for managing trust and coordination within the network. It maintains an immutable ledger of node trustworthiness and network configurations, enabling real-time network reconfiguration based on trust assessments and operational requirements. The control coordination tier ensures that data transmitted across the network adheres to predefined security protocols and operational guidelines, further fortifying the network's integrity.

SABEC utilizes a Two-Tier Consensus mechanism (TTC) to ensure efficient and secure network reconfiguration: ***Trust Evaluation Tier (Data Consensus Stage):*** In this initial tier, nodes perform real-time monitoring of proximal nodes' behaviours using the LTCC and HTCC component protocols. Nodes generate TATs based on observed behaviours, which are then broadcasted to authorized nodes within the upper management network. This tier employs a Lightweight Byzantine Fault Tolerance (LBFT) algorithm to achieve rapid consensus on trust assessments with minimal computational overhead. ***Network Coordination Tier (Decision Consensus Stage):*** The second tier involves the aggregation and validation of TATs through the blockchain's smart contracts. Authorized nodes execute smart contracts to finalize consensus on trust scores and determine necessary network reconfigurations. This tier ensures that only trusted nodes are involved in critical network operations, thereby maintaining the integrity and reliability of the *UAV* network.

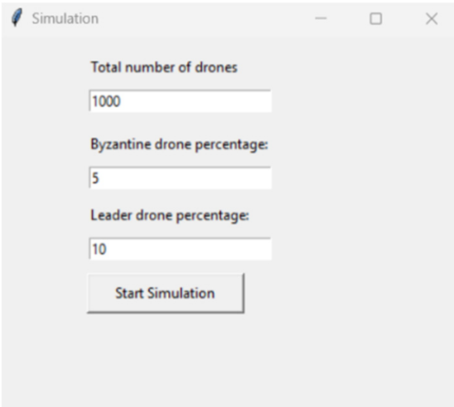

Figure 3: Simulation of the Proposed System.

4 SIMULATION OF THE PROPOSED SYSTEM

To rigorously evaluate the performance and robustness of *SABEC*, comprehensive simulations were conducted using the *NS-3* Network Simulator, a widely recognized tool for modelling and analysing network protocols. The simulation parameters shown in Figure 5. To emulate realistic operational conditions, Windows 11 Home 64-bit 13th Gen Intel Core i7-13650Hx 2.6GHz 32GB RAM were used in the simulation. During the simulation, the behaviour of each node of the network is calculated independently to match the realistic network operation, providing detailed and various statistical data analysis functions.

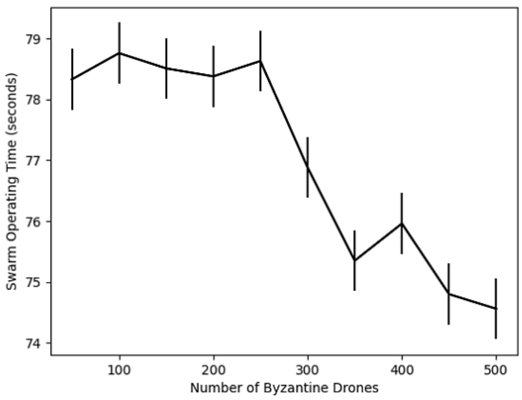

Figure 4: Results of the Simulation.

The simulation environment was meticulously designed to replicate real-world *UAV* mission scenarios, incorporating a range of operational parameters to assess protocol performance under diverse conditions.

Simulation Area	1500 x 1500 m²
Number of UAV Nodes	120
Simulation Duration	300 seconds
Number of Data Links	40
Node Movement Speed	0–35 m/s
Dwell Time	35 seconds
Packet Sending Interval	600 milliseconds
MAC Layer Protocol	IEEE 802.11ac
Wireless Transmission Range	500 meters

Figure 5: Simulation Parameters in NS-3.

Furthermore, the proposed protocol was tested on mission scenarios and the number of *UAV* nodes was selected as 1000 in the simulation experiment. Each testing protocol was run with one hundred scenarios with different random numbers, and the average of all runs was used as the basis for evaluation. The results are shown in the graph in Figure 4. The data obtained shows that Byzantine devices do not affect the proposed system, and the packet transmission speed is quite successful compared to other studies. Various mission scenarios were simulated by incrementally introducing byzantine nodes (ranging from 0 to 35) to evaluate *SABEC*'s resilience against compromised, selfish, and failure-prone nodes. Each scenario was executed thrice with different random node trajectories to ensure statistical validity, and the average results were employed for comprehensive analysis. Malicious nodes exhibited behaviours such as packet dropping, data tampering, and false coordination information dissemination to simulate realistic attack vectors.

SABEC Protocol Implementation

Let $X = \{x_1, x_2, ..., x_n\}$ represent the set of *UAV* nodes in the network, where each x_i contains trust metrics: Message forwarding accuracy (f), Energy consumption (e), and Protocol adherence (p). The *FCM* algorithm minimizes the objective function:

$$J(\mathbf{U},\mathbf{V}) = \sum_{i=1}^{n} \sum_{j=1}^{c} (\mu_{ij})^m \, ||x_i - v_j||^2$$

where is $\mathbf{U} = [\mu_{ij}]$ is the fuzzy membership matrix, $\mathbf{V} = \{v_1, v_2, ..., v_k\}$ represents cluster centers, $m > 1$ is the fuzziness coefficient, $||\mathbf{x}_i - \mathbf{v}_j||$ is the Euclidean distance between node x_i and cluster center v_j . The objective function $J(\mathbf{U},\mathbf{V})$ is the standard formulation used in the *FCM* algorithm. It aims to minimize the weighted sum of squared distances between data points and cluster centers, where the weights are the fuzzy membership degrees raised to the power of ***m***.

Trust Metric Calculation for each UAV node, trust metrics are computed as:

$$T(x_i) = w_1 f + w_2 e + w_3 p$$

Where is w_1, w_2, w_3 are weight coefficients, $0 \leq f,\ e,\ p \leq 1$, $\sum w_i = 1$. The trust value $T(x_i)$ is computed as a weighted sum of normalized trust metrics, which is a common approach in trust assessment models. Ensuring that $\sum w_i = 1$ allows the trust value to remain within a consistent scale. *Algorithm steps as follows. Step 1:* Initialize membership matrix $\mathbf{U}^{(0)}$ randomly FOR each iteration t: Step 2: Calculate cluster centres:

$$\mathrm{v_j} = \frac{\sum_{i=1}^{n}(\mu_{ij})^{m}\,x_i}{\sum_{i=1}^{n}(\mu_{ij})^{m}}$$

Step 3: Update membership values:

$$\mu_{ij} = \frac{1}{\sum_{k=1}^{c}\left(\frac{||x_i - v_j||}{||x_i - v_k||}\right)^{2/(m-1)}}$$

Step 4: Check convergence:

IF $||\mathbf{U}^{(t)} - \mathbf{U}^{(t-1)}|| < \varepsilon$ THEN stop. END FOR

Trust-based Cluster Formation algorithm categorizes nodes into *c* clusters (*c = 3*):

- High-trust cluster (CH): $\mu_{ij} \geq 0.7$
- Medium-trust cluster (CM): $0.3 < \mu_{ij} < 0.7$
- Low-trust cluster (CL): $\mu_{ij} \leq 0.3$

The trust threshold (τ) is dynamically adjusted:

$$\tau(t) = \tau_0 + \alpha\sum(\Delta T/\Delta t)$$

where is τ_0 is the initial threshold, α is the adjustment coefficient, $\Delta T/\Delta t$ represents trust value change rate.

The effectiveness of *FCM* clustering is evaluated using *Silhouette_Score* defined as *(b - a) / max(a,b)* where is *a:* mean intra-cluster distance, *b:* mean nearest-cluster distance. The algorithm incorporates Byzantine fault tolerance by defining the *Trust_Threshold* as *mean(TV) + α * std(TV)* where α is the security parameter (ranging from 1.5 to 2.0), and std represents the standard deviation. Setting the threshold based on the mean and standard deviation allows the protocol to dynamically adjust to the distribution of trust values, enhancing resilience against Byzantine faults. The time complexity is *O(N * C * I * D)* where *N* is the number of nodes, *C* is the number of clusters, *I* is the number of iterations, and *D* is the dimension of the feature vector. The parameters and algorithms presented are correct and appropriately formulated for the implementation of the FCM algorithm within the *SABEC* protocol. They accurately reflect standard methodologies in fuzzy clustering and trust management, and their integration into the *SABEC* framework is logically sound. The detailed steps and formulas provide a robust foundation for dynamic trust assessment, efficient cluster formation, and resilience against Byzantine attacks in *UAV* networks. The fundamental membership verification is based on a fuzzy logic approach combined with blockchain-based validation. The primary membership vector *MV(i)* represents the degree of belonging for each drone *i* to available clusters, expressed as: *MV(i) = [μi1, μi2, ..., μic]* where μij is the membership degree of drone i to cluster j, c is the number of clusters. This vector incorporates multiple parameters including drone positioning, trust metrics, and performance indicators.

The protocol employs a trust-weighted membership strength calculation, *MS(i,j) = μij * w*(T_{ij}) where w(T_{ij}) is the trust-weighted coefficient, T_{ij} represents the trust value of drone *i* in cluster *j*. This formulation ensures that membership assignment is influenced by both fuzzy clustering results and established trust metrics.

The algorithm for Cluster Membership Validation is as follows: Input: Drone D_i , Cluster Set *C* . Output: Validated Cluster Assignment and Proof. First, calculate the Feature Vector *F(i) = [Position(i), Energy(Ū), Trust(i), Performance(i)]*. Next, compute the distance metrics for each cluster C_j in C: *D(i,j)* = || F_i - Centroid(*j*)||. Then, calculate the degrees of membership for each group cluster C_j in C:

$$\mu_{ij} = \frac{1}{\sum_{k=1}^{c}\left(\frac{D_{(i,j)}}{D_{(i,k)}}\right)^{2/(m-1)}}$$

Finally, validate the proof. If $AC_i \geq$ *threshold_membership&ValidateSignature(* $Proof_{(i)}$ *)* and *VerifyConsensus(*$Proof_{(i)}$*)* all hold true, then return *VALID*. Otherwise, return *INVALID*.

Leader Selection Metrics

The primary selection metric is calculated using a weighted composite score SS(i) = α1 * MS(*i,j*) + α2 * TR(*i*) + α3 * PS(*i*) where *SS(i)* is the selection score for drone *i*, *MS(i,j)* is the membership strength in cluster *j*, *TR(i)* is the trust rating, *PS(i)* is the performance score, *α1, α2, α3* are weight coefficients where ∑α = 1. The membership strength *(MS)* is defined as: *MS(i,j) = μij * w(Tij)* where *μij* is the fuzzy membership degree, *w(Tij)* is the trust-weighted coefficient, and *Tij* is the historical trust value. The characteristics features are reflecting drone's belonging degree to specific clusters, incorporating historical performance and accounting for drone distribution. The trust rating calculation *(TR)* is defined as:

$$TR(i) = (\sum_{k=1}^{n} TV(k,i)) / n * \beta$$

where the components are *TV(k,i)* representing the trust value from drone k to drone *i*, *n* is the number of evaluating drones, β is the trust decay factor $(0 < \beta \leq 1)$. Peer evaluation impact, temporal relevance and network consensus are considered. The performance score *(PS)* is defined as:

$$PS(i) = w1 * EC(i) + w2 * CC(i) + w3 * NS(i)$$

where is *EC(i)* is the energy capacity, *CC(i)* is the communication capability, *NS(i)* is network stability, and *w1*, *w2*, *w3* are weight factors. The weight adaptation formula is $\alpha_{new} = \alpha_{current} + \eta * \Delta P$ where η is the learning rate, ΔP represents the performance change. The threshold adjustment is given by $threshold(t+1) = threshold(t) * (1 + \lambda * \Delta E)$ where λ is the adjustment coefficient, ΔE is the environmental change factor.

When the *cluster head selection*, the cluster head score *(CH_score)* is calculated as:

$$CH\_score(i) = SS(i) * (E_{current}/E_{max}) * (1/D_{average})$$

where$E_{current}$ is the current energy level, E_{max} is the maximum energy capacity, and $D_{average}$ is the average distance to cluster members. The role assignment formula is
*Role_fitness(i) = SS(i) * CF(i) * AF(i)* where *CF(i)* is the capability factor, and *AF(i)* is the availability factor.

Proof of Work (PoW) and Leader Election

At the core of *SABEC*'s security mechanisms is the integration of the *PoW* mechanism with leader election. *PoW* serves as a fundamental principle for defending the network and incentivizing legitimate participation. Each node capable of solving a valid *PoW* receives recognition as the legitimate leader. The *PoW* mechanism uses a cryptographic puzzle, which provides fairness in terms of computational effort and fosters scalability among autonomous nodes, deterring collusion. This combined approach improves resilience against Sybil attacks, ensures decentralized governance, and provides more scalability in consensus leadership roles, ultimately contributing to improved security and critical network performance.

The Difficulty Factor *D* is dynamically adjusted to regulate computational effort required by each *UAV*. It is recalculated in response to network changes to ensure fairness and maintain appropriate security provisioning. The expression for *D* is:

$$D = D_{max} \text{ x } \left(\frac{T_{target}}{T_{current}}\right)$$

where T_{target} is the target time for discovering a hash value that meets the condition. This inclusion of a target time ensures the unpredictability of PoW solutions. Nodes solve the difficulty puzzle, and the *UAV* broadcasts the result along with its unique identification to all nearby nodes. Each *UAV* verifies the solution by hashing its assigned identifier, ID_i, the current timestamp t_i, and a generated nonce N_i, as $G = H(ID_i \mid\mid t_i \mid\mid N_i)$. Difficulty verification requires that $G < C_{treshold}$, which is the network difficulty component: $C_{treshold} = C_{max} \text{ x } T_{current}$. This condition ensures that only *UAV*s investing significant computational effort can find a valid solution. Upon finding a valid nonce N_i, the *UAV* broadcasts its solution, including ID_i, t_i, and N_i, to neighboring nodes. Neighboring *UAV*s independently verify the solution by recomputing $C_{treshold}$ and checking the difficulty condition. This step prevents fraudulent claims of *PoW* resolutions. The solution is valid, and the *UAV* proceeds to the next operation of leader election. The criteria to rank and elect the leader involves the highest score in a pre-existing metric calculated as the total assessment, historical performance, operational validity, and peer evaluation: $R_i = \alpha_1 * T_i + \alpha_2 * P_i + \alpha_3 * C_i + \alpha_4 * H_i$ where T_i is trust score of *UAV* node *i*, P_i is performance score, C_i is communication capability, and H_i is historical accuracy. Every authenticated *UAV* node with a verified computational difficulty solution is included in the leadership process, and a unique identifier set $\{ID_i, t_i, N_i\}$ is broadcast to verify identity and ensure consistency.

Security Analysis of SABEC Protocol

The robustness of the Secure and Adaptive Blockchain-Enabled Coordination (*SABEC*) protocol against specific attacks is paramount for ensuring the reliability and security of *UAV* networks. By conducting a comprehensive security analysis, we can elucidate how *SABEC* addresses potential threats such as Sybil attacks, collusion, replay attacks, and Byzantine faults. This analysis highlights the protocol's resilience and the mechanisms by which it safeguards the network's integrity. One of the critical threats in *UAV* networks is the *Sybil attack*, where a malicious entity generates multiple fake identities to gain disproportionate influence over the network. *SABEC* mitigates this risk through a multifaceted approach that combines unique identity verification, blockchain-based identity management, and trust evaluation adjustments. The trust evaluation process incorporates identity verification by assigning lower trust scores to nodes with no or limited history—a common characteristic of newly created Sybil identities. The trust rating for a node i is adjusted using a new identity factor γ_i, where γ_i = 0.5 for new nodes and γ_i = 1 for established nodes. The trust rating is then calculated as:

$$TR(i) = \left(\frac{\sum_{k=1}^{n} TV(k,i)}{n}\right) \text{ x } \beta \text{ x } \gamma_i$$

where $TV(k,i)$ is the trust value from node *k* to node *i*, *n* is the number of evaluating nodes, and β is the trust decay factor.

In addressing *collusion attacks*, where multiple malicious nodes collaborate to manipulate trust assessments or disrupt network operations, *SABEC* employs distributed trust assessment, adaptive weighting mechanisms, and selective consensus participation. Trust evaluations are aggregated from multiple independent nodes, reducing the influence of any colluding group. Each node *k* assesses node *i* and computes $TV(k,i)$. The global trust score *TR(i)* is calculated as:

$$TR(i) = \left(\frac{\sum_{k=1}^{n} TV(k,i)}{n}\right) \text{ x } \beta$$

An anomaly detection mechanism computes the variance σ_i^2 of the trust values for node *i*. If σ_i^2 exceeds a threshold $\theta_{\text{collusion}}$, collusion is suspected, and appropriate measures are taken. Adaptive weighting further diminishes the impact of colluding nodes by weighting trust scores based on the trustworthiness of the evaluating nodes. The weighted trust aggregation is:

$$TR(i) = \left(\frac{\sum_{k=1}^{n} \omega_k \; x \; TV(k,i)}{\sum_{k=1}^{n} \omega_k}\right) \text{ x } \beta$$

where $\omega_k = TR_k$ is the trust rating of node *k*. Nodes with lower trust ratings have less influence on the global trust score, making it difficult for malicious nodes to skew trust evaluations. Moreover, only nodes exceeding a trust threshold $\tau_{consensus}$ participate in the consensus process, limiting the ability of malicious nodes to influence critical network decisions. The trust threshold is dynamically set as: $\tau_{consensus}$ = mean(*TR*) + α * std(*TR*) where α is a security parameter, and std(*TR*) is the standard deviation of trust ratings.

To counter *replay attacks*, where valid messages are maliciously retransmitted to deceive the network, *SABEC* includes timestamps t_i and nonces N_i in messages to ensure freshness. The message structure is: $M_i = \{Data, t_i, N_i, Signature\}$. Recipients verify that the timestamp is within an acceptable window and that the nonce has not been previously used, preventing attackers from replaying old messages.

Addressing *Byzantine faults*, where nodes behave arbitrarily or maliciously, *SABEC* implements a lightweight *Byzantine Fault Tolerance (LBFT)* consensus algorithm. This algorithm ensures that the network can reach consensus even when a fraction of nodes is faulty or malicious. The *LBFT* algorithm tolerates up to f faulty nodes in a network of η nodes, provided that $\eta \geq 3f + 1$. The consensus process involves pre-prepare, prepare, and commit phases, where nodes validate proposals, broadcast verifications, and agree on decisions after receiving sufficient confirmations.

Dynamic leader election, based on trust scores and rotated periodically, prevents any single node from exploiting a leadership position. Key parameters within *SABEC* play a vital role in the protocol's security. The security parameter α affects the sensitivity to trust deviations in threshold calculations, impacting the detection of anomalies and potential attacks. The trust decay factor β controls the influence of past trust evaluations, ensuring that recent behaviors are weighted appropriately in trust assessments. The new identity factor γ_i reduces the trust influence of new nodes, mitigating the impact of Sybil attacks by preventing newly introduced identities from gaining immediate significant influence. The variance threshold $\theta_{\text{collusion}}$ aids in detecting potential collusion by identifying inconsistencies in trust evaluations. The adjustment coefficient κ allows for dynamic adaptation of thresholds in response to environmental changes, ensuring that the protocol remains effective under varying network conditions. The Secure and Adaptive Blockchain-Enabled Coordination (*SABEC*) protocol represents a significant advancement in securing Unmanned Aerial Vehicle (*UAV*) networks. It enhances the integrity and operational resilience through the use of Proof of Work (*PoW*) mechanisms, lightweight hierarchical leader election, and adaptive security policies specifically designed to protect nodes against critical threats. The detailed security threats, such as Sybil attacks, DoS attacks, and Byzantine faults, in the following sections shed light on the intricacies of the *SABEC* framework. The protocol provides significant measures of security and reliability.

5 PERFORMANCE ANALYSIS

The comparative analysis underscores *SABEC*'s superiority in maintaining high performance and reliability under adverse conditions. While traditional protocols like AODV(Tan et al., 2020), OLSR(Proto et al., 2011), and ZRP(Khan et al., 2021) exhibit satisfactory performance in benign environments, their capabilities deteriorate rapidly in the presence of malicious nodes. *SABEC* exhibits superior fault tolerance by dynamically isolating malicious nodes and reconfiguring the network topology. This proactive approach prevents faulty or malicious nodes from disrupting network operations, ensuring continuous and reliable data transmission. Traditional protocols lack such dynamic isolation mechanisms, making them vulnerable to network destabilization under high adversarial conditions. *SABEC* optimizes resource utilization through its hierarchical network structure and efficient consensus mechanisms. By minimizing redundant coordination paths and reducing coordination overhead, *SABEC* ensures that limited *UAV* resources are allocated effectively, enhancing overall network performance and longevity. In contrast, traditional protocols often suffer from excessive routing overhead and inefficient resource allocation, particularly as network size increases. Traditional protocols generally lack integrated security features, rendering them susceptible to various attacks. *SABEC*'s integration of blockchain technology provides robust security enhancements, including immutable trust records and secure consensus operations. This integration effectively mitigates threats such as black hole attacks, gray hole attacks, node impersonation, and collusion, thereby preserving the integrity and reliability of the *UAV* network.

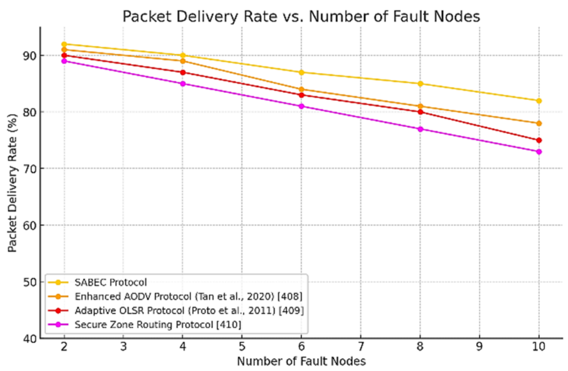

Figure 6: Packet Delivery Rate vs. Number of Malicious Nodes.

The results, depicted in Figure 6, illustrates the Packet Delivery Rate (*PDR*) across different protocols as the number of malicious nodes increases. Initially, AODV (Tan et al., 2020) demonstrates the highest *PDR* in the absence of malicious nodes, closely followed by ZRP(Khan et al., 2021) and *SABEC*. However, as malicious nodes are introduced, the *PDR* of AODV, OLSR, and ZRP declines sharply due to their inability to effectively isolate compromised nodes. In contrast, *SABEC* maintains a high *PDR* even with an increasing number of malicious nodes, thanks to its dynamic trust blockchain-based consensus mechanisms.

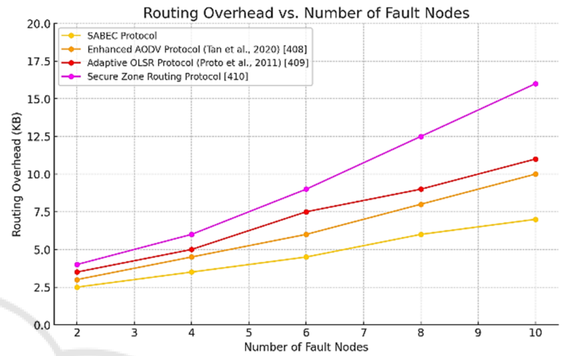

Figure 7: Coordination Overhead vs. Number of Malicious Nodes.

Figure 7 presents the coordination overhead across different protocols under varying numbers of byzantine nodes. Classical protocols like OLSR and AODV exhibit low coordination overhead in benign conditions; however, their overhead surges dramatically as malicious nodes are introduced, primarily due to the proliferation of invalid routing information and continuous route maintenance. Conversely, *SABEC* demonstrates a consistently low and decreasing coordination overhead. This efficiency is achieved through the isolation of untrustworthy nodes and the reliance on a trusted upper management network, which minimizes redundant coordination information and optimizes resource utilization.

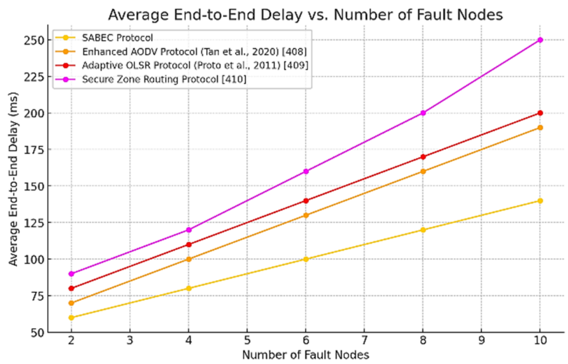

Figure 8: End-to-End Delay vs. Number of Malicious Nodes.

The End-to-End Delay (*E2E Delay*), depicted in Figure 8, is a crucial metric for time-sensitive *UAV* operations. In environments without malicious nodes, ZRP achieves the lowest latency, followed by OLSR and AODV. However, the introduction of malicious nodes leads to a rapid increase in *E2E* Delay for these classical protocols, ultimately causing network instability beyond 30 malicious nodes. *SABEC*, leveraging its trusted coordination mechanisms and hierarchical network structure, maintains low *E2E* Delay even under high adversarial conditions, ensuring timely data delivery essential for mission-critical *UAV* applications.

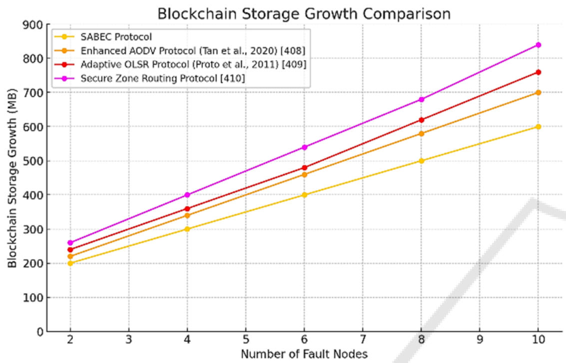

Figure 9: Blockchain Storage Growth Comparison.

Storage and energy efficiency are critical for *UAV* networks, which operate under stringent resource constraints. *SABEC* addresses these challenges through its two-tier consensus mechanism and efficient blockchain integration. Figure 9 demonstrates that *SABEC* significantly reduces blockchain storage growth by retaining only essential consensus results and aggregated trust scores. This approach contrasts sharply with traditional blockchains, which require continuous storage of all transaction data, leading to rapid ledger expansion.

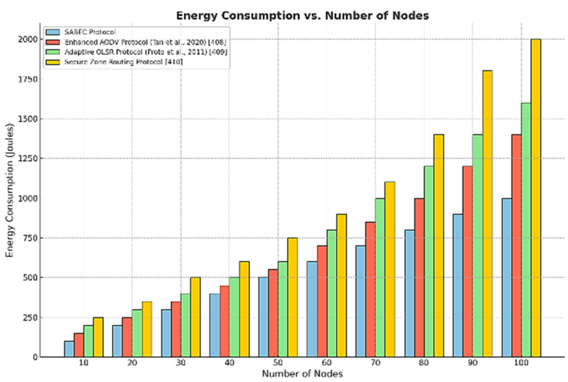

Figure 10: Energy consumption vs. Number of Nodes.

Energy consumption analysis, presented in Figure 10, reveals that *SABEC* outperforms traditional blockchain consensus algorithms such as Proof-of-Work (*PoW*), Proof-of-Stake (*PoS*), and Practical Byzantine Fault Tolerance (*PBFT*). By minimizing computational and communication overhead through trusted coordination and periodic network reconfiguration, *SABEC* ensures sustainable energy usage, thereby extending the operational lifespan of *UAV* nodes. Traditional consensus mechanisms, particularly PoW, incur high energy costs due to their computationally intensive nature, making them less suitable for resource-constrained *UAV* environments.

The comparative performance evaluation of *SABEC* against Enhanced AODV (Tan et al., 2020), Adaptive OLSR (Proto et al., 2011), and Secure ZRP (Khan et al., 2021) highlights its superior resilience, scalability, security, and efficiency under adverse conditions. *SABEC*'s blockchain-based trust mechanisms not only enhance its ability to maintain a high Packet Delivery Rate but also reduce coordination overhead, ensure low End-to-End Delay, and provide scalability, security, and energy efficiency even under challenging conditions. These advantages position *SABEC* as a highly suitable protocol for *UAV* networks where security, efficiency, and responsiveness are paramount.

6 CONCLUSIONS

The comparative analysis The implementation and evaluation of the Secure and Adaptive Blockchain-Enabled Coordination Protocol (*SABEC*) demonstrate its efficacy in enhancing the performance, scalability, and security of *UAV* networks. By integrating blockchain technology with advanced coordination protocols, *SABEC* effectively mitigates coordination overhead, ensures high packet delivery rates, maintains low end-to-end delays, and optimizes energy consumption. The framework's ability to dynamically reconfigure the network in response to changing node states and malicious activities further underscores its suitability for mission-critical *UAV* applications. Simulation results validate *SABEC*'s superior performance compared to traditional coordination protocols, highlighting its resilience and efficiency in complex operational environments. The adoption of a two-tier consensus mechanism and hierarchical network structure ensures that *SABEC* can scale effectively while maintaining robust security and trust management. Future work may explore the integration of machine learning algorithms for predictive trust assessments, further optimization of the consensus mechanism for enhanced energy efficiency, and real-world deployment of *SABEC* in diverse *UAV* mission scenarios to validate its performance in practical applications.

REFERENCES

F. Cunico, F., Aldegheri, S., Avogaro, A., & Boldo, M. (2024). Enhancing safety and privacy in Industry 4.0: The ICE Laboratory case study.12, pp. 154570-154599, 2024. https://ieeexplore.ieee.org/abstract/document/10716394.

Asilian, A., Shahinzadeh, H., & Zanjani, S. M. (2023). The role of microelectronics for smart cities, smart grids, and Industry 5.0: Challenges, solutions, and opportunities. 13th Smart Grid Conference (SGC), Tehran, Iran, Islamic Republic of, 2023, pp. 1-12. https://ieeexplore.ieee.org/abstract/document/10459310.

Yucesoy, Y. F., & Sahin, C. (2024). Object detection in infrared images with different spectra. 2024 International Congress on Human-Computer Interaction. Istanbul, Turkiye, 2024, pp. 1-6. https://ieeexplore.ieee.org/abstract/document/10550753.

Tang, Y., Tian, Y., Lin, Y., & Lv, C. (2024). Guest editorial enabling technologies and systems for Industry 5.0: From foundation models to foundation intelligence. IEEE Transactions on Industrial Informatics, vol. 54, no. 11, pp. 6496-6499. https://ieeexplore.ieee.org/abstract/document/10720572.

Pajany, M., Venkatraman, S., Sakthi, U., & Sujatha, M. (2024). Optimal fuzzy deep neural networks-based plant disease detection and classification on UAV-based remote sensed data. IEEE Transactions, vol. 12, pp. 162131-162144. https://ieeexplore.ieee.org/abstract/document/10740292.

Chung, S. J., Paranjape, A. A., & Dames, P. (2018). A survey on aerial swarm robotics. IEEE Transactions on Robotics. IEEE Transactions on Robotics, vol. 34, no. 4, pp. 837-855. https://ieeexplore.ieee.org/abstract/document/8424838.

Jin, Y., Minai, A. A., & Polycarpou, M. M. (2003). Cooperative real-time search and task allocation in UAV teams. 42nd IEEE International Conference on Decision and Control, pp. 7-12 Vol.1. https://ieeexplore.ieee.org/abstract/document/1272527.

Queralta, J. P., Taipalmaa, J., Pullinen, B. C., & Sarker, V. K. (2020). Collaborative multi-robot search and rescue: Planning, coordination, perception, and active vision. IEEE Access, vol. 8, pp. 191617-191643. https://ieeexplore.ieee.org/abstract/document/9220149.

Yang, J., Wang, Y., Hang, X., & Delahaye, D. (2024). A review on airspace design and risk assessment for urban air mobility. IEEE Access, vol. 12, pp. 157599-157611. https://ieeexplore.ieee.org/abstract/document/10718279.

Lou, T., Wang, Y., Yue, Z., & Zhao, L. (2024). Multi-UAV collaborative trajectory planning for 3D terrain based on CS-GJO algorithm. Complex System Modeling and Simulation, vol. 4, no. 3, pp. 274-291. https://ieeexplore.ieee.org/abstract/document/10737157.

Du, P., Xiao, T., Cao, H., & Zhai, D. (2024). AI-based UAVs 3D coverage deployment in 6G-enabled IoV networks for Industry 5.0. IEEE Transactions on Consumer Electronics. https://ieeexplore.ieee.org/abstract/document/10716736.

Dogan, H. (2023). Protecting UAV-Networks: A Secure Lightweight Authentication and Key Agreement Scheme. 2023 7th International Conference on Cryptography, Security and Privacy (CSP), Tianjin, China, 2023, pp. 13-21. https://ieeexplore.ieee.org/document/10235922.

Wang, B., Xing, Y., & Wang, N. (2024). Monitoring waste from unmanned aerial vehicle and satellite imagery using deep learning techniques: A review. IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing. https://ieeexplore.ieee.org/abstract/document/10738392.

Silva, F. A., Barbosa, V., Lima, L. N., Sabino, A., & Rego, P. (2024). Efficient strategies for unmanned aerial vehicle flights: Analyzing battery life and operational performance in delivery services using stochastic models. IEEE Access, vol. 12, pp. 144544-144564. https://ieeexplore.ieee.org/abstract/document/10646335.

Amarcha, F. A., Chehri, A., & Jakimi, A. (2024). Drones optimization for public transportation safety: Enhancing surveillance and efficiency in smart cities. IEEE World Forum on Public Safety Technology (WFPST), pp. 153-158. https://ieeexplore.ieee.org/abstract/document/10607062.

Salim, N. (2024). A comprehensive review on the design and development of drones for diverse applications: Classifications, applications, and design challenges. SSRN. http://dx.doi.org/10.2139/ssrn.5002521.

Chen, X., Xiao, Z., Cheng, Y., & Hsia, C. C. (2024). FireHunter: Toward proactive and adaptive wildfire suppression via multi-UAV collaborative scheduling. IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Vancouver, BC, Canada, 2024, pp. 1-2. https://ieeexplore.ieee.org/abstract/document/10620862.

Alsamhi, S. H., Shvetsov, A. V., & Shvetsova, S. V. (2022). Blockchain-empowered security and energy efficiency of drone swarm consensus for environment exploration. IEEE Transactions on Green Communications and Networking, vol. 7, no. 1, pp. 328-338. https://ieeexplore.ieee.org/abstract/document/9852392.

Jin, C., Yao, H., Mai, T., Xu, J., & Zhang, Q. (2024). A resource-efficient content sharing mechanism in large-scale UAV named data networking. IEEE/ACM Transactions on Networking. https://ieeexplore.ieee.org/abstract/document/10716865.

Jiang, C., Fang, Y., & Zhao, P. (2020). Intelligent UAV identity authentication and safety supervision based on behavior modeling and prediction. IEEE Transactions on Industrial Informatics, vol. 16, no. 10, pp. 6652-6662. https://ieeexplore.ieee.org/abstract/document/8960477.

Liang, Q., Hu, Y., Yan, Y., & Zhou, L. (2024). Drone target detection based on improved YOLOv5s algorithm. IEEE

43rd Chinese Control Conference, pp. 8357-8362. https://ieeexplore.ieee.org/abstract/document/10661446.

Khan, M. A., Kumar, N., Alsamhi, S. H., & Barb, G. (2024). Security and privacy issues and solutions for UAVs in B5G networks: A review. IEEE Transactions on Network and Service Management. https://ieeexplore.ieee.org/abstract/document/10737101.

Jiang, H., Li, N., & Yi, P. (2024). PUBA: A physical undirected backdoor attack in vision-based UAV detection and tracking systems. International Joint Conference on Neural Networks (IJCNN), pp. 1-8. https://ieeexplore.ieee.org/abstract/document/10650950.

Sedjelmaci, H., & Senouci, S. M. (2017). A hierarchical detection and response system to enhance security against lethal cyber-attacks in UAV networks. IEEE Transactions on Aerospace and Electronic Systems, vol. 48, no. 9, pp. 1594-1606. https://ieeexplore.ieee.org/abstract/document/7890467.

Bertrand, S., Raballand, N., & Lala, S. (2024). Handling ground risks for road networks in UAS specific operations risk assessment (SORA). International Conference on Unmanned Aircraft Systems (ICUAS), pp. 850-857. https://ieeexplore.ieee.org/abstract/document/10556970.

Kundu, J., Alam, S., Das, J. C., Dey, A., & De, D. (2024). Trust based Flying ad-hoc network: A survey. IEEE Access, vol. 12, pp. 99258-99281. https://ieeexplore.ieee.org/abstract/document/10574806.

Fang, H., Wang, X., Xiao, Z., & Hanzo, L. (2022). Autonomous collaborative authentication with privacy preservation in 6G: From homogeneity to heterogeneity. IEEE Network, vol. 36, no. 6, pp. 28-36. https://ieeexplore.ieee.org/abstract/document/9839653.

Hughes, I., Pupo, A., Wynd, J., & Thurlow, Z. (2024). Securing the unprotected: Enhancing heartbeat messaging for MAVLink UAV communications. IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PACRIM), pp. 1-6. https://ieeexplore.ieee.org/abstract/document/10690216.

Li, T., Zhang, J., Obaidat, M. S., Lin, C., & Lin, Y. (2021). Energy-efficient and secure communication toward UAV networks. IEEE Internet of Things Journal, vol. 9, no. 12, pp. 10061-10076. https://ieeexplore.ieee.org/abstract/document/9560132.

He, D., Yang, G., Li, H., Chan, S., & Cheng, Y. (2020). An effective countermeasure against UAV swarm attack. IEEE Network, vol. 35, no. 1, pp. 380-385. https://ieeexplore.ieee.org/abstract/document/9183792.

Abishu, H. N., Sun, G., & Yacob, Y. H. (2024). Multi-agent DRL-based consensus mechanism for blockchain-based collaborative computing in UAV-assisted 6G networks. IEEE Internet of Things Journal. https://ieeexplore.ieee.org/abstract/document/10726599.

Sun, A., Sun, C., Du, J., & Chen, C. (2024). AoI optimization for UAV-assisted wireless sensor networks. IEEE International Conference on Communications, pp. 1487-1492. https://ieeexplore.ieee.org/abstract/document/10615615.

Tan, X., Zuo, Z., Su, S., Guo, X., & Sun, X. (2020). Research of security routing protocol for UAV communication network based on AODV. Electronics, 9(8), 1185. https://www.mdpi.com/2079-9292/9/8/1185.

Proto, F. S., Detti, A., Pisa, C., & Bianchi, G. (2011). A framework for packet-droppers mitigation in OLSR wireless community networks. 2011 IEEE International Conference on Communications (ICC), 1–6. https://ieeexplore.ieee.org/document/5963001.

Khan, I. U., Shah, S. B. H., Wang, L., Aziz, M. A., Stephan, T., & Kumar, N. (2021). Routing protocols & unmanned aerial vehicles autonomous localization in flying networks. International Journal of Communication Systems, 34(9), e4885. https://onlinelibrary.wiley.com/doi/abs/10.1002/dac.4885.