drones

MDPI

Article

*i*BANDA: A Blockchain-Assisted Defense System for Authentication in Drone-Based Logistics †

Simeon Okechukwu Ajakwe *,‡, Ikechi Saviour Igboanusi ‡, Jae-Min Lee and Dong-Seong Kim *

Department of IT Convergence Engineering, Kumoh National Institute of Technology, Gumi 39177, Republic of Korea; ikechisaviour@kumoh.ac.kr (I.S.I.); ljmpaul@kumoh.ac.kr (J.-M.L.)

* Correspondence: simeonajlove@gmail.com (S.O.A.); dskim@kumoh.ac.kr (D.-S.K.)

† This paper is an extended version of our conference paper: BANDA: A Novel Blockchain-Assisted Network for Drone Authentication. In Proceedings of the Fourteenth International Conference on Ubiquitous and Future Networks (ICUFN), Paris, France, 4–7 July 2023.

‡ Current address: ICT Convergence Research Centre, Kumoh National Institute of Technology, Gumi 39177, Republic of Korea.

Abstract

Background: The increasing deployment of unmanned aerial vehicles (UAVs) for logistics in smart cities presents pressing challenges related to identity spoofing, unauthorized payload transport, and airspace security. Existing drone defense systems (DDSs) struggle to verify both drone identity and payload authenticity in real time, while blockchain-assisted solutions are often hindered by high latency and limited scalability. Methods: To address these challenges, we propose *i*BANDA, a blockchain- and AI-assisted DDS framework. The system integrates a lightweight You Only Look Once 5 small (YOLOv5s) object detection model with a Snowball-based Proof-of-Stake consensus mechanism to enable dual-layer authentication of drones and their attached payloads. Authentication processes are coordinated through an edge-deployable decentralized application (DApp). Results: The experimental evaluation demonstrates that *i*BANDA achieves a mean average precision of 99.5%, recall of 100%, and an F1-score of 99.8% at an inference time of 0.021 s, validating its suitability for edge devices. Blockchain integration achieved an average network latency of 97.7 ms and an end-to-end transaction latency of 1.6 s, outperforming Goerli, Sepolia, and Polygon Mumbai testnets in scalability and throughput. Adversarial testing further confirmed resilience to Sybil attacks and GPS spoofing, maintaining a false acceptance rate below 2.5% and continuity above 96%. Conclusions: *i*BANDA demonstrates that combining AI-based visual detection with blockchain consensus provides a secure, low-latency, and scalable authentication mechanism for UAV-based logistics. Future work will explore large-scale deployment in heterogeneous UAV networks and formal verification of smart contracts to strengthen resilience in safety-critical environments.

Keywords: anti-drone; decentralized application; smart contract; AI-on-edge; secure drone delivery; DDS; PoS

Academic Editors: Peiying Zhang and Athanasios V. Vasilakos

Received: 23 July 2025
Revised: 17 August 2025
Accepted: 18 August 2025
Published: 20 August 2025

Citation: Ajakwe, S.O.; Igboanusi, I.S.; Lee, J.-M.; Kim, D.-S. *i*BANDA: A Blockchain-Assisted Defense System for Authentication in Drone-Based Logistics. *Drones* **2025**, *9*, 590. https://doi.org/10.3390/drones9080590

1. Introduction

Drone use for priority-based logistics has become increasingly popular in recent years [1]. However, several security concerns jeopardize the viability of civilian drone use [2]. Lately, there have been multiple accounts of heightened interference and airspace breaches due to the controversies surrounding drone use and its offspring, also referred to as unmanned aerial vehicles (UAVs) [3]. Data from the US Federal Aviation Authority

(FAA) reveals that between January 2016 and December 2022, a total of 14,178 incidents involving UAV-related airspace security violations occurred across the country [4]. This statistic represents nearly a 200% increase compared to the 8124 cases reported in 2015 [3]. Drone defense systems (DDSs) are cyber–physical systems (CPSs) that operate in hard real-time over fault-tolerant networks (FTNs) to oversee and monitor drone operations and activities against invasive and malicious uses, including espionage, network jamming, retaliation attacks, and spying [5].

Despite advancements in DDS technologies, several security challenges persist in drone operations, particularly within logistics. These include verifying and ensuring accountability in drone package delivery [6]; managing drone user identity theft [7]; preventing drone communication hijacking; ensuring drone user authentication [8,9]; authorizing drone operators [10]; and enabling dynamic drone engagement and neutralization based on environmental impact assessments [5]. Specifically, payload security, which entails the timely verification of drone identity and cargo ownership, is critical to curtail identity theft, smuggling, and the risk of nuclear weapon carriage, among other threats, and maintain air freight security [11]. These challenges imply that the deployment of artificial intelligence (AI)-driven defense strategies to ensure safe and secure drone-based logistics may not be as effective as they could be [5,12], particularly when it comes to anonymity concerns brought on by flaws in current security architectures. Thus, the intelligence and integrity of UAV defense systems depend largely on the underlying cognitive and cybersecurity models, which serve as both eyes and brains to perceive and respond to the myriad of drone-based logistic scenarios around them and within their network.

To provide smart and safe aerial logistics operations, legacy-based DDS (empowered by AI and IoT) takes between 100 ms to 1700 ms to authenticate the validity of a drone within its network range before initiating an appropriate counter-response [13]. Albeit with several security loopholes. Safe and secure drone-based logistics operations could be revolutionized by integrating blockchain technology into the DDS networks, which provide a secure, traceable, decentralized, and tamperproof platform for sending, storing, and verifying the source of sensitive data [14]. However, this additional blockchain layer in the DDS network can result in increased DDS complexity and response delay while improving authentication validity. Due to the necessity of balancing security, speed, and scalability—a problem that has persisted in blockchain-assisted designs—the application of blockchain technology in DDS is still in its infancy.

Few attempts have been made to use blockchain and related technologies to address these enduring DDS security problems. Most of these works focused mainly on cybersecurity issues with little or no relevance to drone-based logistics and supply chain security, as captured in Table 1. At present, issues related to latency (speed) in real-time transmission and communication, especially in detecting and addressing security vulnerabilities caused by malicious drone deployment, continue to be drawbacks of blockchain-based drone authentication methods.

Authors [5,15,16] created trusted computing and AI-based methods for drone authentication while they are in flight. Additionally, to provide safe drone authentication, authors [17–19] used AI–blockchain technology for drone user-route evaluation as a means of verifying a drone operator's authority, localization, and legality inside a given jurisdiction. These frameworks, however, lacked transparent mutual authentication, had privacy concerns, complicated sensor-fusion processes, and did not address tethered items to the drone. They also incurred overhead costs. Also, blockchain-based drone ownership verification frameworks were developed by authors [20–22] to bring transparency and improve trustworthiness in verifying drone users and owners. However, because of their overhead costs, these frameworks are unsuitable for DDS to offer optimal security because they are

porous and vulnerable to malicious cyberattacks. Additionally, authors [23,24] demonstrate in their work that the integration of blockchain technology into an Internet of Drones (IoD) greatly curtails cyberattacks. However, none of these works addressed the issue of drone payload authentication and security, which is critical for safe aerial-based logistics.

Table 1. Comparative analysis of related drone authentication approaches.

Reference	Detection	Package Verification	Blockchain Used	Authentication Time	Gaps
[18]	Acoustic-based	×	×	N/A	No blockchain integration; vulnerable to spoofing and lacks data integrity checks.
[19]	RF-based	×	PoA	N/A	Does not authenticate attached packages; limited blockchain scalability.
[25]	RF-based	×	×	N/A	Lacks transparency and content-level verification; does not support logistics payload security.
[17]	RF-based	×	×	N/A	Does not support package or object authentication; lacks decentralized validation.
[26]	×	×	×	N/A	Lacks explicit security/authentication measures; no blockchain to ascertain transparency.
[27]	×	×	×	Low (lightweight symmetric key exchange)	No integration of AI and blockchain for safe logistics operation.
iBANDA (Ours)	**Visual + Lidar-based**	✓	**Advanced PoS (Avalanche)**	**Avg. 97.72 ms (Net), 1606.6 ms (DApp)**	**Provides full drone + package authentication with low-latency, scalable blockchain; supports real-time response and decentralized verification.**

N/A = Not Applicable; × = Not considered; ✓ = Considered

To authenticate the package source during drone product delivery, authors [28] presented a secured distribution of protected material in information-centric networking. However, it lacks decentralization and insufficient mobility support. In a similar vein, the authors in [5] developed a multi-modal system for object verification and neutralization, which combines visual object detection and assisted learning to tackle decentralization in drone package verification. These investigations, however, lacked transparency, were unable to validate sealed contents, and did not consider blockchain technology. These results indicate that due to the complexity and legality involved in validating the authenticity of drone-based packages, blockchain technology has been rarely deployed in DDS. Hence, because the perceived threat posed by drone usage depends on the drone and the attached object [12], this research is motivated by the need to guarantee safe and smart drone-based logistics by enhancing the capacity of DDS via the incorporation of blockchain technology into its operations.

Thus, an inventive DDS that offers optimal security against malevolent drone deployment for logistics can be realized by utilizing the data processing power of AI algorithms and the immutable nature of blockchain technology. Therefore, this study is driven by the need to address the speed (latency), safety, and security capacity of current DDS architectures by fusing lightweight blockchain technology with AI models. It will ensure safe drone operations for value chain logistics with minimal security risks. In addition to the traditional drone authentication method, an off-chain transaction mechanism is implemented to verify the network's timeliness and efficiency. To the best of our knowledge, no prior research has leveraged blockchain technology to encapsulate package delivery status verification, operator authorization, legality, dynamic scenario-specific neutralization, and drone user authentication. This research's novelty results from this.

Although recent works have explored practical applications of autonomous aerial vehicles (AAVs) and UAVs in different domains, none of these works focused on drone-based logistic operations. For instance, the authors in [26] proposed a performance analysis and optimization design of AAV-assisted vehicle platooning in a non-orthogonal multiple access (NOMA)-enhanced Internet of Vehicles (IoV) environment, focusing on communication resource allocation and cooperative control performance. Similarly, [29] presented an AAV

swarm authentication and key agreement scheme based on Latin square design, emphasizing lightweight symmetric key generation for fast authentication in swarm scenarios.

While these works are valuable, our proposed iBANDA framework addresses a different set of challenges and application contexts. Unlike [26], which targets communication and control optimization for vehicular platoons, iBANDA focuses on securing UAV-based logistics and smart mobility missions operating in adversarial environments. Additionally, in contrast to [29], which employs a centralized symmetric cryptographic approach, iBANDA integrates a dual-layer security mechanism combining AI-based anomaly detection with blockchain consensus (Proof-of-Stake Snowball) to achieve distributed, explainable, and attack-resilient authentication. Notably, our framework incorporates a weather-friendly and resilient AI technique to ensure transparency in security decisions and provides quantitative resilience analysis against Sybil and GPS spoofing attacks—features not covered in the aforementioned works. These differences position iBANDA as a complementary contribution to the UAV security literature, bridging the gap between performance-optimized UAV networking and lightweight cryptographic authentication by delivering a trustworthy, reproducible, and empirically validated security architecture for UAV-based mobility and logistics applications.

The key contributions of this study are as follows:

- We developed a strategy for thorough permission, authentication, and verification of drones and the packages (payloads) before dynamic neutralization is activated.
- Then, we created a decentralized application that operates on the edge and built a transparent blockchain network to validate authentication settings.
- Finally, we integrated the created blockchain network and application into the drone defense system to verify its authorization and validity for use as a smart mobility vehicle.

The uniqueness of the proposed blockchain-enhanced DDS framework is captured in Table 1, highlighting its superiority over existing methods. Unlike the existing methods that primarily rely on RF or acoustic signals for drone detection and offer limited or no consideration for payload authentication, the proposed iBANDA framework provides a comprehensive, real-time drone and package verification system. It uniquely integrates AI-based visual and Light Detection and Ranging (LIDAR) sensing with lightweight blockchain authentication, enabling dual-layer validation of both the drone identity and the legitimacy of its attached object. iBANDA leverages the Avalanche consensus (an advanced PoS algorithm) to maintain high scalability, rapid transaction validation (97.72 ms network time), and low computational cost—far surpassing the performance of PoA- and PoW-based approaches. This dual-modular strategy ensures that any discrepancies between the drone and its declared payload are immediately flagged, triggering appropriate neutralization responses. By combining decentralized trust, rapid consensus, and multi-modal AI inference, iBANDA offers a more resilient, scalable, and secure solution for drone-based logistics, making it highly suitable for deployment in safety-critical and time-sensitive smart city environments.

In this paper, Section 2 addresses the authentication problem formulation; Section 3 covers the methodology and system design; Section 4 presents and discusses the results; while the article is concluded in Section 5. All acronyms and symbols used in this paper can be found in the table in the Abbreviations section.

2. Soundproof Authentication Formulation

Modeling a DDS to address comprehensive and dynamic drone operation challenges, often referred to as "NP-problems," is inherently complex regarding logistical considerations. This is because various interlining system components and controlled parameters must be intuitively taken into account before a final, time-sensitive automated deci-

sion or response is made. Several AI models have been used in this field of study [3,5]. The "DRONET" AI model, which we built in our earlier work [12], is utilized in this work for drone detection and associated item identification. Additionally, it adopts the "ALIEN" framework in the works of authors [5] for the scenario-specific neutralization response after proper authentication has been carried out. Following the theory of the kinematic model for an autonomous mobile robot with Ackermann steering, a drone typically operates within a 2D coordinate system, as illustrated in Figure 1.

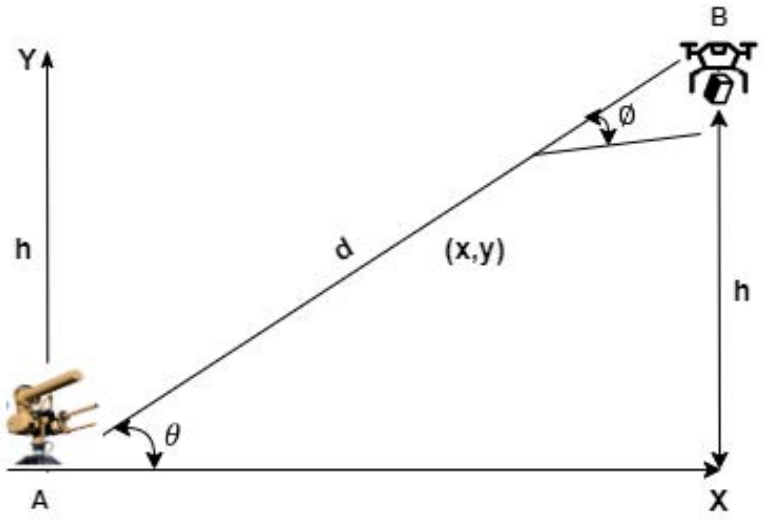


Figure 1. Motion analysis of a standard DDS authentication process for actively engaging a drone within its detection range.

By leveraging the drone's registration details, transmitted GCS data (for drones controlled via GCS), and other collected sensor parameters, a typical DDS connected through the cloud can detect drones within its range. It can identify the attached object, measure the drone's distance or proximity ($\overline{AB}$), estimate its altitude ($\overline{BX} \equiv \overline{AY}$), determine the direction of arrival (θ), and calculate its speed (ϕ). By using these obtained parameters, a secure network such as a blockchain can be used to verify a drone's condition. Equation (1) defines the DDS engagement for drone authentication challenges mathematically as a linear transformation function:

$$D \mapsto d_X, \tag{1}$$

Here, d_X denotes the authentication input variables or parameters, specifically all pairs $(x, f(x))$ for $x \in X$, which are required to define the overall drone authentication function as outlined in Equation (2).

$$D = \begin{bmatrix} A_1 & A_2 & \cdots & A_n \\ B_1 & B_2 & \cdots & B_n \\ C_1 & C_2 & \cdots & C_n \end{bmatrix}_{t+1} \tag{2}$$

Let A represent the drone–user status, B the drone–source status, C the drone–package status, $t+1$ the current timestamp, and n the total number of drones within detection range.

In legacy-based DDS engagements, the primary goal is typically to optimize the drone authentication target function (D) for each input variable (x) while adhering to constraints related to time (t) and other network and control parameters (ψ), as specified in Theorem (1).

Theorem 1. *At any moment i, the dynamic involvement of a DDS (D) in authenticating a specific logistics drone (d)—accounting for its varying distance/proximity (s) and altitude (h) in real time*

(t) over a secure cloud network—is determined by the drone's user state (d_u), source identity (d_i), and package delivery status (d_p).

This is described in Equation (3).

$$D_l = f_d(u_t, i_t, p_t), \tag{3}$$

Let D_l represent the Legacy DDS engagement determinant at the current timestamp, while u_t, i_t, and p_t denote the control input vectors corresponding to the drone user state, source, and package status at the same timestamp. By extending Equation (3) to incorporate drone proximity to the DDS—considering both distance and altitude—we obtain the following:

$$D_l = \oint_{k=1}^{n} \{d_{u,t}, d_{i,t}, d_{p,t}\} \cdot \{d_{st}, d_{ht}\}, \tag{4}$$

where d_{st} and d_{ht} are the drone proximity values to the DDS. Generally, the latency of a drone response time can vary based on the given situation and ranges from 100 to 1700 milliseconds (ms) [13].

Integrating blockchain technology into the existing DDS network, as illustrated in Figure 2, will inevitably increase system complexity and potentially reduce responsiveness. This is because greater complexity tends to negatively impact scalability and speed.

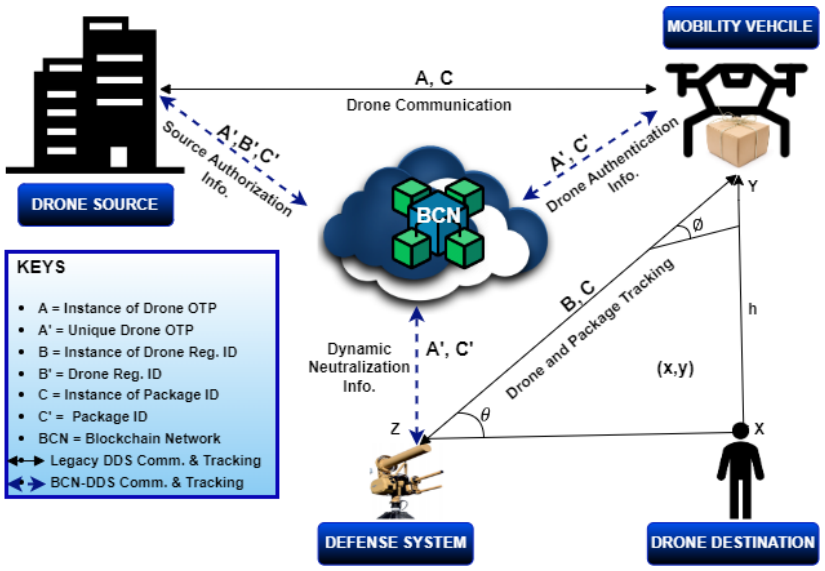


Figure 2. Secured and safe drone logistics operation highlighting the centrality of blockchain technology for trustworthy authentication.

As a result, the objective function of the blockchain-enabled DDS engagement ($\mathtt{D}_\uparrow$) is designed to optimize the legacy DDS system's capacity for drone authentication ($\mathtt{D}$) across all input variables (x) while considering time (t) and other network and control constraints (ψ). The goal is to achieve this optimization with minimal computational overhead while enhancing security. To address the computational challenges and improve responsiveness, a lightweight blockchain model is adopted. This model supports the DDS network ($\mathtt{D}_\uparrow$) and operates independently of the conventional legacy-based approach.

By introducing blockchain, the drone authentication problem in Equation (4) is transformed into Equation (5):

$$D^{\uparrow} = \oint_{k=1}^{n} \{d'_{u,t}, d'_{i,t}, d'_{p,t}\} \cdot \{d_{st}, d_{ht}\}, \tag{5}$$

Let $d_{u_t'}$ (A′) represent the Unique Drone OTP that distinguishes it from others, $d_{it}^{'}$ (B′) denote the Drone Registration ID used to trace the drone's source, and $d_{p_t}^{'}$ (C′) signify the Package ID employed for tracking and verifying the legitimacy and destination of the conveyed item. A discrepancy in the response capability and behavior for dynamic engagement between $\mathtt{D}_1$ and $\mathtt{D}_\uparrow$ within a specified timeframe signals a security breach, potentially caused by malicious drone activity. Thus, $\mathtt{D}_\uparrow \neq \mathtt{D}_1$ points to an authentication failure in the legacy DDS's dynamic engagement mechanism, while $\mathtt{D}_\uparrow \equiv \mathtt{D}_1$ indicates a secure and reliable engagement process.

Hence, a robust authentication system designed to enhance defense security against the malicious use of drones in smart mobility is outlined as follows:

$$D_{\max} = \sum\left(D^{\uparrow} - D_l\right) \equiv \eta_b, \tag{6}$$

The response time for conventional legacy DDS authentication is limited to a maximum threshold ranging from 100 to 1700 milliseconds.

Traditionally, before the drone begins its flight, information such as the drone's source registration details, user/operator identity, and package delivery data is sent to the cloud, represented by $\mathtt{A}', \mathtt{B}', \mathtt{C}'$ in Figure 2, which the DDS uses for authentication during the flight. During smart mobility operations, the legacy DDS ($\mathtt{D}_1$) engages the target drone by obtaining this information ($\mathtt{A}, \mathtt{B}, \mathtt{C}$) through GCS sensing. This process relies on its underlying defense technology, which is considerably inadequate. In contrast, the proposed blockchain-assisted DDS ($\mathtt{D}_\uparrow$) retrieves all relevant drone information within line of sight from the cloud and validates its authenticity using the BCN before responding automatically. If, at any point, there is a discrepancy between the parameters of the legacy DDS ($\mathtt{D}_1$) and the blockchain-assisted DDS ($\mathtt{D}_\uparrow$), a perceived danger analysis and corresponding procedure are initiated based on the specific scenario.

3. *i*BANDA Framework

The proposed iBANDA framework enhances the drone defense system (DDS) by integrating artificial intelligence (AI) for object detection and blockchain for secure, real-time authentication. It comprises three core layers: the AI-based Detection (AD) layer, the Altruistic Blockchain Authentication (AB) layer, and the adaptive response (AR) layer. These components work in tandem to ensure that both the drone and its payload are verified before allowing operation and to trigger dynamic neutralization when a discrepancy is detected. Ensuring that algorithmic decision-making aligns with ethical standards is essential for advancing autonomous vehicle technology and ensuring its long-term viability. In terms of system modeling, the authors based their work on the following assumptions and ethical considerations:

- The drone detection and attached object identification algorithm is intact and controlled by an AI object detection model, as seen in the works of [12];
- The scenario-specific neutralization response framework is intact as proposed in our previous work, the ALIEN model [5];
- There is an overseeing organization that governs airspace activities, acting as the primary authority for drone operations and security [4];
- Each drone employed for smart mobility is licensed to operate and properly registered in the network, classified either as a freight operator or a hobby drone user with the relevant regulatory authority [30];
- The participating registered drone users and logistics operators serve as validators for the mining process in the blockchain network.

The system design, including input, processing, and output, is summarized in the logic diagram shown in Figure 3. The AD layer handles physical security via object detection of the drone and the delivered payload, while the AB layer carries out authentication. The AB security model is built on a public blockchain framework operating on an Ethereum Virtual Machine (EVM) network. It employs a consensus protocol that is robust, scalable, decentralized, and governed by intelligent and lightweight smart contracts (SM) automation. The security system processes data as input, authenticates it through mining activities within a specified block time, and produces feedback via a decentralized application (DApp). The DApp output serves as the feedback that the AR uses to initiate an appropriate neutralization response, which could be active or passive, by activating jammers, spoofers, drone shooters, and other mechanisms. With the AD, AB, and AR layers working congruently, the proposed scheme ensures physical and cybersecurity issues associated with drone logistics are tackled.

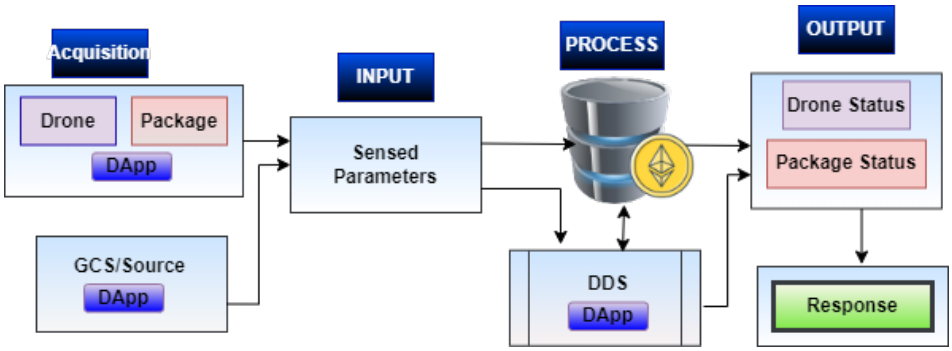


Figure 3. Proposed DDS logic diagram highlighting flow of activities during operation.

3.1. AD: Cognitive Object Detection Layer

The AI-based detection module was designed using a modified and improved lightweight You Only Look Once version 5 small (YOLOv5s) that is deployed on the edge with a speedy detection capacity and minimal storage/complexity. To optimize the AD model, a 128 × 128 input size was used, ONNX quantization was applied for deployment, and the model was pruned by removing unneeded layers and filters. This enabled the model to be deployed on NVIDIA Jetson Nano. The choice of YOLOv5s over newer versions (such as YOLOv8, 9, and 10) as the underlying model for the object detection layer is that YOLOv5s is lightweight and optimized for real-time detection on devices with limited compute and thermal budgets. Also, it has more mature and stable support for ONNX and TensorRT, which are critical for fast inference on NVIDIA Jetson devices.

3.2. AB: Altruistic Blockchain-Based Authentication Layer

To address security and scalability challenges, iBANDA employs a lightweight blockchain layer powered by a Snowball-based consensus algorithm—a variant of Proof of Stake (PoS). This consensus method ensures fast, decentralized decision-making by querying a random subset of validator nodes and updating preferences based on repeated agreement.

3.2.1. System Authentication Data

The system data comprises the drone user and operator information as well as the package delivery information. The characteristics of system data are captured in Table 2.

The drone input includes several components: a time-synchronized one-time password (OTP), a unique security token (D_{mac}) corresponding to the drone's MAC address, and a hash value—specifically, a one-time password (D_{otp})—sent by the source to the blockchain network. Additionally, it includes the GCS signal information (D_{gcs-x}, D_{gcs-y})

used to verify the MAC address and the drone's source, a soft token for package delivery ($P_{st} \equiv P_{otp}$) sent by the source to the cloud, and an RFID tag as a hard token ($P_{ht} \equiv P_{gcs}$) attached to the delivery package. The RFID tag can be detected and retrieved by the DDS from the drone while in flight, within its detection range, as shown in Figure 4. These six data points form the system input parameters that the DDS uses to authenticate the drone before determining the appropriate neutralization action.

Table 2. System data features.

SNo.	Category	Drone	Package Delivery
1.	Hard Security Token	D_{mac}	$P_{ht} \equiv P_{gcs}$
2.	Soft Security Token	D_{otp}	$P_{st} \equiv P_{otp}$
3.	Source GCS Signal	D_{gcs-x}	
4.	Operator GCS Signal	D_{gcs-y}	

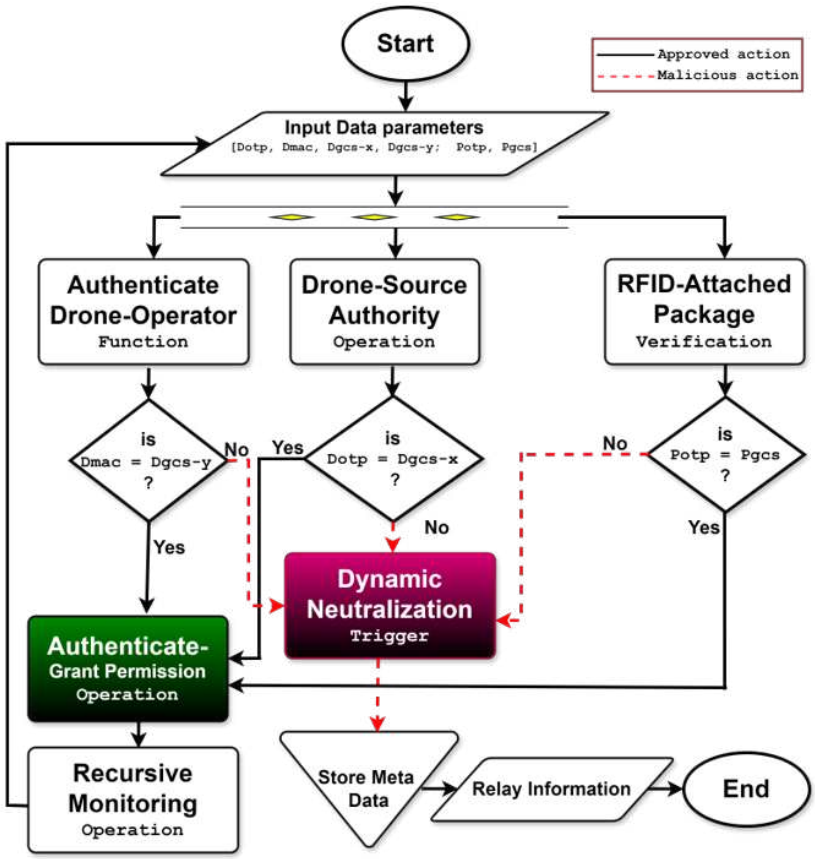


Figure 4. Flowchart of DDS authentication illustrating the package and drone verification process.

Although Figure 4 focuses on the logical authentication sequence, the actual implementation in iBANDA integrates multiple safeguards against the mitigation of Man-in-the-Middle (MITM) attacks. All UAV–GCS–blockchain communications are secured via mutual TLS/DTLS 1.3 with blockchain-validated public keys, ensuring that both endpoints are authenticated before any data exchange. Session keys are derived from blockchain-signed credentials, and each authentication message includes a nonce and timestamp to prevent replay or tampering. Additionally, the AI-based anomaly detection layer monitors flight behavior for deviations that may indicate control interception, triggering re-authentication and blockchain verification.

3.2.2. Scalable Decentralized Security

Typically, drones have resource-constrained hardware characteristics and demand lightweight, computationally efficient, and cost-effective security mechanisms. Therefore, we adopted a Snowball-based consensus algorithm (the Avalanche) for drone authentication. This algorithm has the unique advantage of gaining speed, scalability, energy efficiency, and adaptive security that can resist various vulnerabilities in drone network operations, such as Sybil, collusion, and distributed denial of service (DDoS) attacks [30]. The Avalanche uses the repeated sub-sampled voting technique (an advanced proof of stake (PoS) algorithm) to determine whether a transaction coming from a node will be accepted or rejected based on a random subset of validator nodes' preferences. Each queried participating validator replies with the transaction that it thinks should be accepted or preferred. The consensus does not include an invalid transaction. A preferred choice is made when a sufficient majority of the validators' sampled reply with the same preferred transaction. $\uparrow$ represents the number of validators required for consideration as the sufficient majority, while $\downarrow$ represents the confidence threshold, i.e., the number of consecutive rounds required to reach consensus. In this study, the decentralized authentication security uses a snowballing algorithm as the building block of the Avalanche consensus, as summarized in Theorem 2 and Algorithm 1.

Theorem 2. *Given a set of n validators in the network, a transaction is authenticated when a quorum of α validators (out of a random sample k) repeatedly agree on the same preference for β consecutive rounds. This mechanism ensures resilience to Sybil attacks and guarantees that authentication is both robust and efficient.*

Algorithm 1: Snowballing Consensus Algorithm for Drone Authentication

```
Initialize preference ← legit-drone
Initialize counter ← 0
while Not decided do
    Sample k validator nodes
    Each validator votes for the preferred transaction
    if votes for same preference ≥ α then
        if current preference matches previous preference then
            Increment counter
        end
        else
            Set new preference
            Reset counter to 1
        end
    end
    else
        Reset counter to 0
    end
    if counter > β then
        decide(preference)
    end
end
```

3.3. Snowballing Authentication Algorithm

The snowballing mechanism used in iBANDA (see Algorithm 1) is designed to balance speed and security in resource-constrained drone networks. It ensures that multiple nodes must continuously and repeatedly agree on a transaction before it is committed, minimizing the risk of false acceptance.

As seen in Algorithm 1, the initial transaction preference is set as $\texttt{legit} - \texttt{drone}$. Until a transaction has been decided, the sample size (k) is queried, and each validator is requested to make a preference. If α or more validators give the same response, the response is then accepted as the new `choice`, but when the old choice is the same as the old choice, the counter `consecutive Successes` is incremented. However, if the new `choice` differs from the old `choice`, the counter is set to 1. Finally, if no response gets to α, the counter is set to 0. All the validators repeat this process until the value of α has the same response β times in a row. If a participating validator decides a drone to be $\texttt{legit} - \texttt{drone}$, each validator using the same protocol accepts the drone as $\texttt{legit} - \texttt{drone}$. To prevent malicious actors from participating in the drone network as validators and thereby compromising the authentication process, each participating node that acts as a validator must bond (stake) something valuable and must be frequently queried by other participating nodes to validate its correctness and sufficient responsiveness.

3.3.1. Parameterizing Snowball for iBANDA

In our deployment, we ground the symbolic parameters of Snowball as follows. Let k denote the number of validators sampled per round. We set the quorum threshold to $\alpha = \lceil 0.70k \rceil$ and the confidence threshold to $\beta = 5$ consecutive rounds. This choice reflects a practical balance between responsiveness and robustness under adversarial conditions: in our Sybil-resilience experiments with 50 validators and up to 50% malicious identities, $\alpha{=}\lceil 0.70k \rceil$, $\beta{=}5$ sustained sub-110 ms consensus completion time, and kept the false acceptance rate below 2.5%. (See Table 9 and Figure 15 for FAR/TRR/CCT trends under Sybil and GPS-spoofing tests.) Meanwhile, the aggregate authentication pipeline preserves low network time (mean 97.72 ms) and $\approx$1.6 s end-to-end DApp latency across increasing loads (Table 7). To support other operating points, Table 3 provides a heuristic map from mission objectives to recommended (α, β) ranges.

Table 3. Heuristics for choosing Snowball parameters (α, β) in iBANDA. Here, k is the sampled validator set per round. Higher α and β improve robustness against Sybil/collusion at the cost of added confirmation time.

Objective	Quorum Size α	Rounds β	Expected Effect
High responsiveness	$\lceil 0.50k \rceil \ldots \lceil 0.60k \rceil$	3…4	Faster decisions; lower latency; modest robustness
Balanced (default)	$\lceil 0.70k \rceil$	5	∼97–110 ms CCT; FAR $\lesssim$2.5%; ∼1.6 s end to end
High robustness	$\lceil 0.80k \rceil \ldots \lceil 0.90k \rceil$	6…7	Strong Sybil/collusion tolerance; higher confirmation time

3.3.2. Convergence Probability and Byzantine Resistance

Following the Avalanche/Snowball analysis in [31], the probability of converging to the correct value in the presence of f Byzantine validators is bounded below by

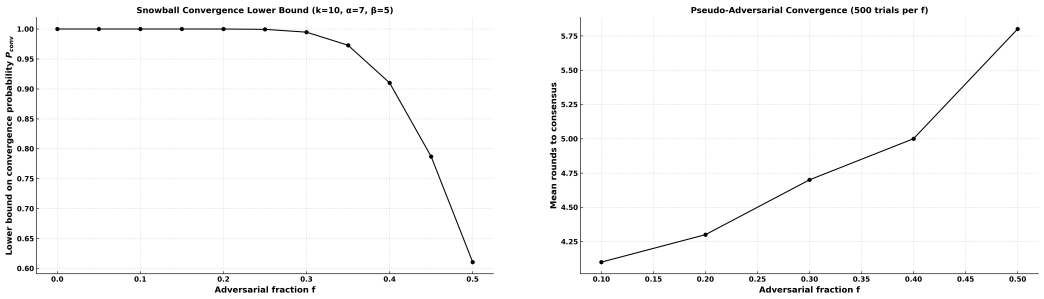
$$P_{\text{conv}} \geq 1 - \left(\frac{\sum_{i=\alpha}^{k} \binom{k}{i} p^i (1-p)^{k-i}}{\sum_{i=0}^{k} \binom{k}{i} p^i (1-p)^{k-i}} \right)^{\beta}, \tag{7}$$

where $p = 1 - \frac{f}{n}$ is the honest node fraction, n is the total validator population, k the number of sampled validators per round, α the quorum size, β the required consecutive

agreement rounds, and f the number of Byzantine nodes. For our operational setting ($n = 50$, $k = 10$, $\alpha = \lceil 0.70k \rceil = 7$, $\beta = 5$) and $f/n \leq 0.5$, this bound yields $P_{\text{conv}} \geq 0.997$.

Snowball tolerates Byzantine actors provided the adversarial fraction is below the metastability threshold (≈51% for uniform random sampling), above which coordinated adversaries could bias the quorum. Our parameterization leaves a margin between α/k and the honest node fraction p, ensuring that adversaries cannot consistently obtain quorum without controlling both a validator majority and the random sampling process. This guarantees both low-latency convergence and high robustness in realistic UAV authentication deployments.

Figure 5a visualizes the lower bound in Equation (7), while Figure 5b shows that the empirical rounds-to-convergence under pseudo-adversarial load closely track the theoretical trend and remain within ≤6 rounds for $f \leq 0.4$ (and ≤7 rounds at f = 0.5 in 98.2% of trials).



(**a**) (**b**)

Figure 5. Theoretical and empirical convergence of Snowball under iBANDA parameters. The left panel plots the conservative lower bound from Equation (7); the right panel shows observed mean rounds from Table 10. (**a**) Lower bound on P_{conv} vs. adversarial fraction f for k = 10, α = 7, β = 5; (**b**) pseudo-adversarial convergence: mean rounds to consensus over 500 trials per f.

In practice, this authentication logic is deployed via smart contracts on a blockchain network. Prior to a drone flight, key credentials such as drone ID, operator ID, and payload ID are submitted to the blockchain. During flight, the DDS compares real-time data from the drone with the blockchain records. If all data match, the drone is permitted to continue. However, any mismatch triggers an immediate alert, and the system can execute a proportional neutralization response—e.g., rerouting, disabling, or immobilizing the drone—depending on the severity of the discrepancy. This real-time dual-layer verification ensures that unauthorized drones or payloads are not allowed to enter sensitive airspace or perform logistics operations. By combining the high accuracy of AI-based object detection with the transparency and immutability of blockchain, iBANDA significantly reduces risks such as spoofing, smuggling, or unauthorized surveillance.

To initiate the verification and authentication process for the drone package, the procedure starts with a transaction request from the drone source to the BCN (refer to Figure 2), notifying that a drone is about to begin a delivery operation within the network, along with its $\mathtt{D_{mac}}$ and $\mathtt{D_{otp}}$ sent to the cloud. Following this, the drone source initiates a transaction that includes a fee. Miners (validators) in the network perform mining according to Algorithm 1 and generate a `preference`. The DDS then retrieves this hash value and cross-checks it with the GCS signal data ($\mathtt{D_{gcs-x}}$) received from the logistics company. If the values match, the process is authenticated and continues recursively as long as the drone remains in flight, unless a discrepancy arises. This process is illustrated in the flow chart in Figure 4. The gas cost and time required for completing the transaction are also recorded.

The system performs a one-time comparison between the $\mathtt{D_{mac}}$ value retrieved from the cloud and the $\mathtt{D_{gcs-y}}$ value obtained from the GCS for disparity and authenticates them ac-

cordingly. Additionally, it conducts a one-time cross-check of the package delivery data (P_{st}) from the cloud against the P_{ht} value sensed by the system. These three processes—drone-source authorization, drone operator authentication, and package verification—are carried out concurrently in real time, with each authentication metric contributing to the final decision of whether to permit or deny the drone's operation. If any discrepancies are found, the DDS triggers an appropriate neutralization response based on factors such as the environmental impact assessment and data from detection routines (e.g., detection range, visual object representation, accuracy, etc., from [5,12]). The DDS response, also known as neutralization via kinematic countermeasure, can be either destructive (e.g., shooting down the drone) or non-destructive (e.g., disarming or re-routing) through methods such as jamming or spoofing [5]. The procedure for scalable authentication is summarized in Algorithm 2.

Algorithm 2: DDS Scalable Continuous Authentication D_{max}

Input: Acquire variables: D_{otp}, D_{mac}, D_{gcs-x},...P_{otp};
Execute Edge server and interact with blockchain layer;
while *True* **do**
    Call `Drone Source Authority` (D_{otp}=D_{gcs-x});
    Call `OperatorAuthentication` (D_{mac}=D_{gcs-y});
    Call `RFID − Attached Package Verification` (P_{otp}=P_{gcs});
    if Steps 4, 5, and 6 == ***True*** **then**
        Authenticate & Grant `Permission − to − fly` ;
        Operate `Recursive Monitoring`;
    end
    else
        Trigger `Dynamic Neutralization`;
        Relay & store $\texttt{Drone}_{\texttt{information}}$;
    end
    return D_{max}
end

3.4. Formal State Machine and Petri Net of iBANDA Authentication and Response

To formally capture the discrete operational logic of the iBANDA authentication pipeline, we model the process as a deterministic Finite State Machine (FSM) and an equivalent Petri net. These models reflect both normal and anomalous UAV behaviours during the Pre-authentication → Authentication → Neutralization flow. The FSM in Figure 6 defines the sequential control logic, while the Petri net (in Figure 7) explicitly represents concurrent credential verification and β-round Snowball consensus accumulation.

The FSM is defined as follows:

$$M = (Q, \Sigma, \delta, S_0, F)$$

where

- Q = {S0: Pre-authentication, S1: Acquire_Credentials, S2: Credential_Checks, S3: Consensus_Wait, S4: Authenticated, S5: Reauthenticate, S6: Neutralization_Decision, S7: Handover_Stop, S8: Log_Relay, S9: Error}.
- Σ = {e_acq, e_src_ok, e_op_ok, e_pkg_ok, e_all_ok, e_missing, e_mismatch, e_consensus_yes, e_consensus_no, e_anomaly, e_recover, e_log, e_handover, e_fatal}.
- S_0 = Pre-authentication.
- F = {Authenticated, Neutralization_Decision, Handover_Stop, Error}

The transition function δ is provided in Table 4.

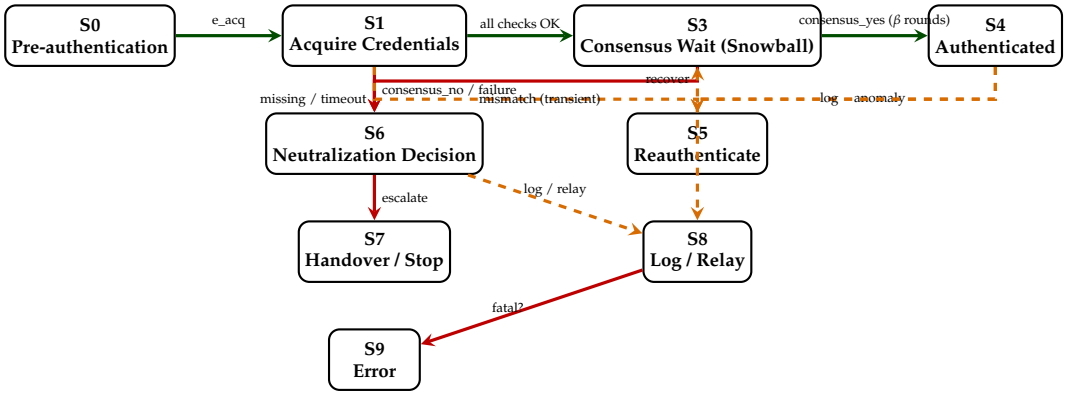


Figure 6. Color-coded FSM for iBANDA authentication and response. Green: normal success path; Orange dashed: anomaly/recovery paths; Red: failure/neutralization paths. Guards use Algorithm 2 and Snowball quorum parameters (α, β).

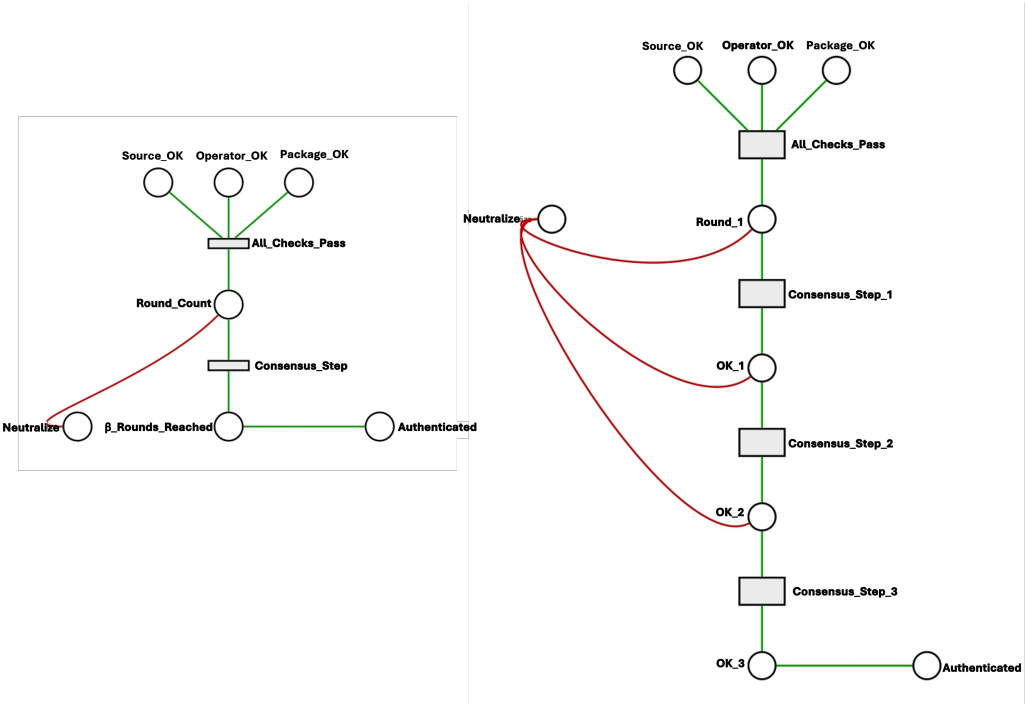


Figure 7. (**Left**) High-level Petri net for iBANDA: green = success flow; red = failure path to neutralize. (**Right**) Expanded Petri net for $\beta = 3$: green = successful round progression; red = failure path to neutralize.

Guards in the FSM are directly derived from the Algorithm 2 verification steps ($Dotp \equiv Dgcs\text{-}x, Dmac \equiv Dgcs\text{-}y, Potp \equiv Pgcs$) and Algorithm 1 Snowball consensus quorum parameters (α, β). Any missing credentials, data mismatches, or consensus failures cause deterministic transitions to the Neutralization_Decision state, where the Autonomous Response (AR) layer determines proportional countermeasures. Any missing credentials, data mismatch, or consensus failure transitions the system into a Neutralization_Decision state where the AR layer computes proportional countermeasures. Runtime anomalies detected by the AD layer cause re-authentication or neutralization, depending on severity.

Table 4. FSM state transitions for iBANDA authentication and response.

From State	Event/Guard	To State	Action
S0 (Pre-authentication)	e_acq	S1 (Acquire_Credentials)	Collect Dotp, Dmac, Potp, Dgcs-x, Dgcs-y, Pgcs
S1 (Acquire_Credentials)	All checks OK: $(Dotp \equiv Dgcs\text{-}x) \wedge (Dmac \equiv Dgcs\text{-}y) \wedge (Potp \equiv Pgcs)$	S3 (Consensus_Wait)	Submit tx to BCN; start Snowball rounds
S1	Missing credential or timeout	S6 (Neutralization_Decision)	AR selects hold/neutralize; log event
S1	Equality mismatch (non-severe)	S5 (Reauthenticate)	Request resend or degraded path
S3 (Consensus_Wait)	consensus_yes (β rounds)	S4 (Authenticated)	Permit_to_fly; continue monitoring
S3	consensus_no/quorum fail	S6 (Neutralization_Decision)	Escalate
S4 (Authenticated)	e_anomaly	S5 (Reauthenticate) or S6	Severity-based routing
S5 (Reauthenticate)	e_recover	S3 (Consensus_Wait)	Retry consensus
Any	e_log	S8 (Log_Relay)	Write on-chain and local log
Any	e_handover	S7 (Handover_Stop)	Transfer to authority
Any	e_fatal	S9 (Error)	Safe shutdown

Petri Net Representation

The equivalent Petri net (Figure 7(left)) models *parallel verification* of the three credentials (`Source_OK`, `Operator_OK`, and `Package_OK`). A *synchronisation transition* (`All_Checks_Pass`) fires only when all three tokens are present, feeding into the *Snowball* β-round consensus subnet. Similarly, Figure 7(left) captures the expanded equivalent Petri net model for verification, synchronization transition, and neutralization decision.

The formal model explicitly models fault-handling paths for missing data, mismatches, or consensus failures. Also, it enables formal verification via model checking for safety properties (e.g., absence of deadlocks and bounded neutralization delay). Finally, it provides a bridge for concurrency analysis through Petri net reachability. (Green arrows = standard success flow (fast visual recognition); orange dashed arrows = anomaly/recovery handling (non-fatal issues); red arrows = failure, neutralization, or fatal error paths.)

3.5. AR: Smart Contract Design and Dapp Implementation Interface

The adaptive response (AR) layer relies on the intelligent feedback from the AB smart contract design. The smart contract (SM) for automating actions (blockchain transactions) required in the drone network was developed using Solidity within our "pure chain" framework, with a summary of the implementation parameters highlighted in Table 5.

Table 5. Implementation parameters.

Parameter	Description
Network	Ethereum Virtual Machines (EVMs)
Consensus	Repeated sub-sampling voting; Proof of Stake (PoS)
Smart contract language	Solidity (0.7.6+committ.7338295f)
Dapp Language	Dart (flutter)
Device	MacBookAir
Chip/RAM	M1/16GB
OS	macOS Ventura (Version 13.2)

The entity-relationship diagram (ERD) in Figure 8 illustrates the association or relationship between detected drone parameters, the packaged delivery parameters, the delivery company parameters, and the DDS for authentication and authorization operations.

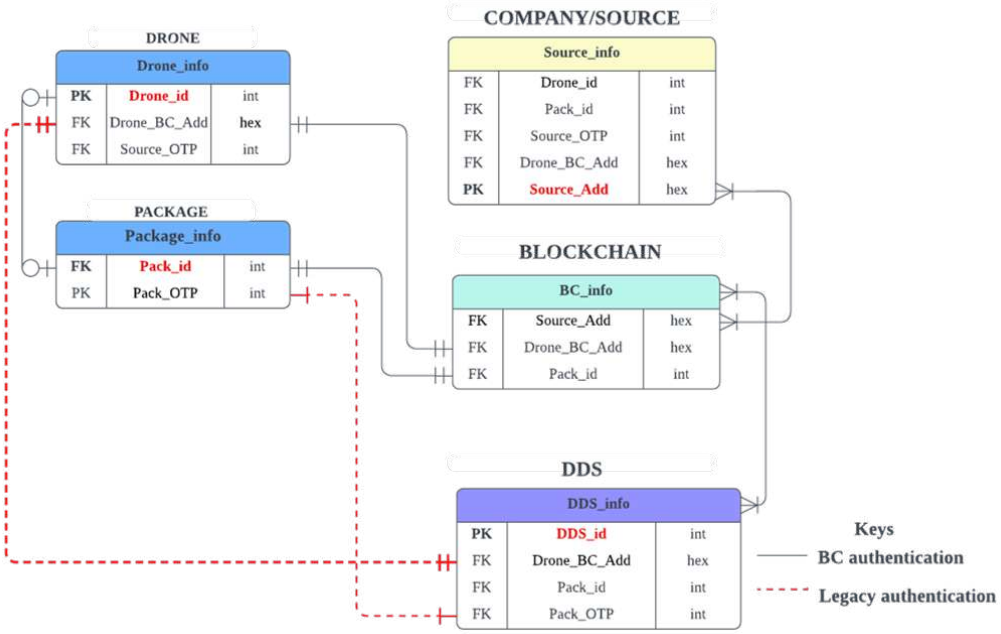


Figure 8. The *i*BANDA entity relationship between the drone, the attached object, the source, and the DDS during operations.

The ERD shows that the DDS operations are in two phases, the BC-assisted and the legacy approach, and run concurrently, as indicated by the thick and broken lines. The DDS legacy operations utilize the DRONET prediction and network-based parameters (`Drone − id`) to detect the drone while using a lidar scanning technique (`Pack − OTP`) to identify the attached object. On the other hand, the BC-assisted side (`BC − info`) utilizes the unique drone address (`Drone − BC − Add`) made available by the drone source (`source − info`) to the blockchain network to authenticate the drone. Also, it uses the unique package ID (`pack − id`) from the source to the blockchain network to perform a one-time verification of the attached package on the drone. The outcome of the authentication determines the appropriate incapacitation response that is triggered.

Figure 9 is the underlying decentralized application (Dapp) interface, designed on the Remix integrated development environment (IDE) where the input parameters are entered, retrieved, processed, and transmitted in the network. The "orange" color parameters (such as `companyDrone`, `companyGood`, `companyPeriod`, etc.) with their underlying variable names represent the acquired system input. In contrast, the "dark-blue" color parameters (such as `antiDroneDrone`, `antiDroneGood`, etc.) represent the system output by the Dapp interface. These automated parameters are manipulated and utilized to authenticate the drone and the attached package. To test the system robustness and efficiency, the proposed framework was deployed on different Ethereum virtual machines (EVMs) with varying consensus algorithms such as Proof of Authority (PoA), Proof of Stake (PoS), and Proof of Work (PoW) to ascertain the authentication speed, scalability, energy-efficiency, and adaptive security. Overall, the *i*BANDA framework (as the underlying BC-assisted network for drone authentication) interacts with the DRONET model [12] (for drone and attached object detection) and the ALIEN strategy [5] (for scenario-specific response) to confirm the status of a drone operation in real time. The DDS uses this information to respond intuitively and rapidly to prevent the deployment of invasive drones.

Figure 9. The Dapp interface of the smart contract deployed on Remix IDE, along with the smart contract processes for authorizing drones and authenticating the attached package to the drone.

4. Results and Discussion

This section presents a detailed analysis and discussion of the performance of the proposed iBANDA framework. First, Section 4.1 briefly discusses the AI model detection performance as an integral part of the proposed system. Then, Section 4.2 presents a detailed analysis and discussion of the security-speed and responsiveness (latency) of the blockchain side of the system. Thereafter, Section 4.3 focuses on the security–scalability analysis (resource efficiency) of the *i*BANDA framework, with emphasis on authentication speed, scalability, energy efficiency, and adaptive response. Finally, Section 4.5 compares the proposed system performance with other blockchain networks and drone authentication approaches to validate its uniqueness.

4.1. Performance Evaluation I: AI-Model Drone and Package Detection

The adopted AI algorithm is a modified YOLOv5n (tiny) object detection model with a path aggregation network (PANET) to improve the detection of tiny objects. Refer to [5] for details of the algorithm configuration. The results in Table 6 summarize the performance of the adopted model against conventional deep learning object detection algorithms and variants of the YOLO algorithm using various performance evaluation metrics.

Table 6. AI-model detection performance.

Models	Overall Model Performance (Detection and Package Identification)					
	mAP (%)	R (%)	F1 (%)	Time (fps)	Rel. Loss	Space Used GFLOPS
SqueezeNet	83.41	85.10	88.50	0.030 s	0.0921	22.50
GoogleNet	89.55	88.75	89.10	0.035 s	0.0685	24.10
VGG-16	89.25	83.20	86.10	0.039 s	0.0781	26.50
MobileNet V2	74.50	72.05	74.01	0.476 s	0.0951	18.40
ResNet	89.53	90.10	89.81	0.040 s	0.0983	21.70
v3	97.20	89.50	95.50	0.016 s	0.0426	23.30
v5s	96.50	100.0	98.10	0.022 s	0.0440	16.50
p2+v5	98.30	100.0	99.10	0.024 s	0.0587	19.10
fpn+v5	100.0	70.80	82.90	0.023 s	0.0421	16.20
Yolov8	93.40	84.00	88.50	0.019 s	0.0652	29.70
Adopted model	**99.50**	**100.0**	**99.80**	**0.021 s**	**0.0370**	**16.10**

At a glance (see Figure 10), the adopted AI model achieved a superior throughput of 16.10 GFLOPS. Giga Floating Point Operations Per Second (GFLOP) measures how many billion numerical operations a model can process each second. In this context, it indicates

the computational efficiency of the AI model, highlighting its suitability for real-time drone detection on resource-constrained edge devices. This implies that the computational cost of the model is relatively low compared to heavier deep learning models (e.g., YOLOv8 and ResNet). Also, the adopted model achieved a mean average precision (mAP) of 99.50%. It indicates the system reliably distinguishes drones and payloads from the background with extremely low false-positive errors. Furthermore, it has a sensitivity (R) of 100%, meaning that the model did not miss any positive cases in the test set (zero false negatives). In other words, every drone and payload that was supposed to be detected was successfully detected. With a rational detection behavior (F1-score) of 99.80%, the model makes balanced and reliable decisions. This implies that it is neither biased toward over-detection (many false positives) nor under-detection (many false negatives) compared to other state-of-the-art models. The model had an inference time of 0.021s, implying that the model needs 21 milliseconds per image/frame to make a prediction. Thus, $[\frac{1}{0.021}]$ *is* $\approx$ 47.6 frames per second (fps), meaning that the system can process roughly 47 frames per second, which is faster than the 30 fps of standard video, fast enough for real-time UAV defense applications. Finally, the model had a minimal prediction error (loss) of 0.0370, better than other models, including the recent YOLOv8 model. The result indicates the model makes very few mistakes when identifying drones and payloads. Thus, the model is not just memorizing the training data but also predicting well on unseen UAV and payload images.

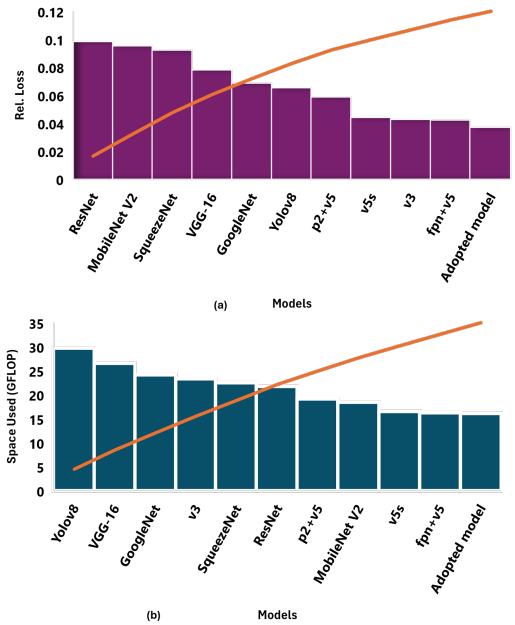


Figure 10. Reliability and efficiency graph of different AI models for drone and attached object detections, highlighting their performance with (**a**) prediction error performance and (**b**) memory usage for prediction.

Overall, across all metrics, the adopted model achieved better reliability and resource-usage efficiency (minimal cost) than other object detection models. This validates its choice as the preferred underlying intelligent cognition engine to meet the hardware-resource constraint characteristics of DDS and to support the blockchain authentication procedure. The samples of detected drones and attached object recognition highlighted in Figure 11 show the prediction performance of the adopted model as the underlying AI inference models that work in conjunction with the proposed *i*BANDA algorithm.

Figure 11. Samples of real-time drone detection and attached objects recognition and elicitation by DRONET [12] and ALIEN [5] based on the VisioDect [32] dataset showing high prediction precision and sensitivity on different climatic scenarios necessary for the *i*BANDA authentication and eventual neutralization.

4.2. Performance Evaluation II: Authentication Capacity, Reliability, and Security Analysis

This section presents a detailed evaluation of the iBANDA framework, focusing on latency, throughput, scalability, computational cost, and overall authentication effectiveness across various network conditions.

4.2.1. Latency Analysis

Specifically, the system authentication capacity is analyzed based on the timeliness (speed)/latency of the DDS to ascertain the status of the drone(s) and their attached object while guaranteeing security. This is because latency in DDS is critical due to its time-sensitive operational context. The model receives a continuous flow of data from the logistics company and stores it on the blockchain network. The drone monitors the blockchain network and fetches the data value from the blockchain smart contract. Two types of latency were evaluated:

- **Read latency (μt_1)**: Time between data submission to the network and initial acknowledgment.
- **Transaction latency (μt_2)**: Total time taken for authentication to be completed and validated across the blockchain.

The results in Table 7 show the latency performance of the *i*BANDA based on the adopted algorithm (Avalanche) on different rounds of streams of data (the number of transactions) representing different drones in the network whose legitimacy is confirmed by the system before triggering the appropriate neutralization response.

The "Network Time" (R_1) in Table 7 represents the average time taken between multiple logistics companies (drone sources) to send the data into the network for mining to take place. That is,

$$\overrightarrow{NT} = \frac{1}{N}\sum_{n=1}^{N}\delta\left(NT_2 - NT_1\right) \equiv \Delta NT, \tag{8}$$

where N = the number of drones and package delivery received; NT_1 = time taken to receive the signal from the Dapp, and NT_2 = time taken to complete mining in the network. For instance, it took the Avalanche an average ($\underrightarrow{\alpha}$NT) of 99 ms to handle eight drone

mining requests. A similar time was achieved as the number of drones participating in the network increased, as seen in Figure 12.

Table 7. Latency performance of iBANDA with increasing drone requests.

Sno.	Number of Drones	Network Time (ms)	Dapp Time (ms)
1	8	99	2293
2	9	99	1595
3	10	99	1566
4	11	99	1563
5	12	101	1539
6	13	99	1519
7	14	102	1602
8	15	96	1502
9	16	97	1525
10	17	93	1472
11	18	91	1497
	Average:	97.72	1606.63

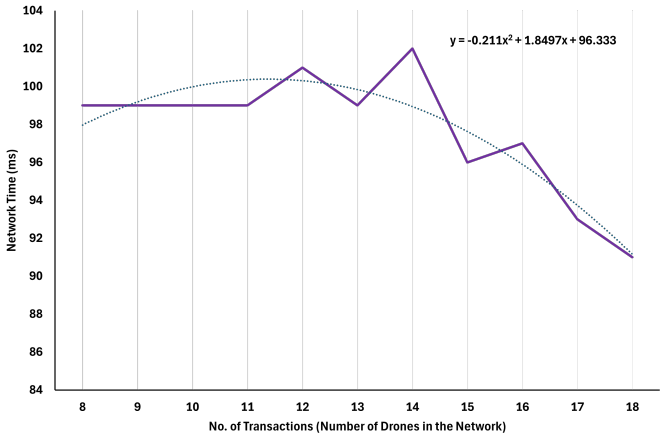


Figure 12. Network time graph of proposed algorithm showing the time taken to handle mining requests with an increased number of participating drones in the network. The dash line is the trend of the network time with increase in number of drones.

Succinctly, the adopted algorithm (Avalanche Fuji Testnet) takes between 91 ms and 101 ms to receive requests from the Dapp and complete mining to confirm the legitimacy of a detected drone and its package delivery. Thus, after 11 rounds of testing (with 18 drone transactions), the system had an average of 97.7 ms to validate and complete mining. Furthermore, it can be deduced from Figure 12 that an increase in the number of drones participating in the blockchain network had little or no effect on the time taken to carry out the authentication. Although the network time peaked at 102 ms when the number of participating drones was 14, it gradually steepened from 96 ms to 91 ms with an increased number of drones, indicating an improved latency. Thus, this confirmed that the proposed approach has good authentication latency and scalability with an increased number of drones in the network.

On the other hand, "Dapp Time" (T_1) is the overall time that the smart contract receives the company's data, allows the mining to take place ($\overrightarrow{NT}$), and gets feedback from the network on the result of the mining, which is then released to the DDS. This means the time needed for authentication by the *i*BANDA-controlled DDS to verify and authenticate a drone's legitimacy and its attached object through the blockchain network, as illustrated in Figure 13.

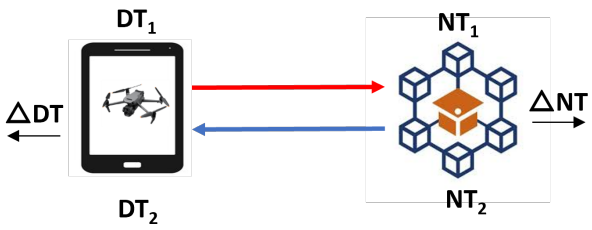


Figure 13. Illustration of time taken for transaction mining and completion of authentication from the decentralized (Dapp time) and the Network.

Equation (9) expresses the Dapp time mathematically:

$$\overrightarrow{DT} = \frac{1}{N}\sum_{n=1}^{N}\delta(DT_2 - DT_1) \equiv \Delta DT, \tag{9}$$

where $\mathtt{N}$ = the number of drones and package delivery received; $\mathtt{DT_1}$ is the time when the Dapp sent the data to the BC network; and $\mathtt{DT_2}$ is the time when the Dapp received the feedback from the blockchain network.

As seen in Table 7, it takes an average Dapp time of 2293 ms to complete the authentication of eight drones. Also, it can be observed that as the number of drones (the number of transactions) increased, there was a significant decrease in Dapp time, with the least being 1497 ms to complete the authentication of 18 drones (see Figure 14).

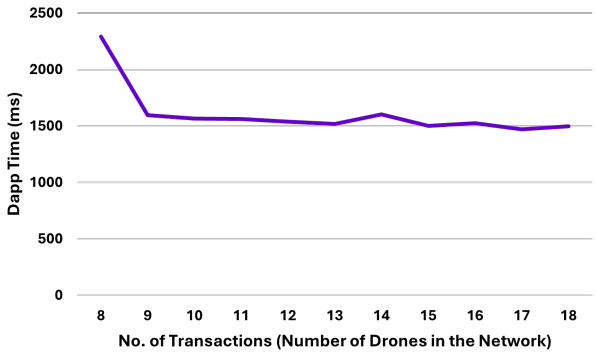


Figure 14. Dapp time graph of the proposed algorithm showing the time taken to confirm a drone's and attach object legitimacy with an increased number of participating drones in the network.

Thus, after 11 rounds of testing, it takes an average of 1606.6 ms (≈1 s) to confirm the drone's legitimacy and report to the DDS for a situational-based response. These results indicate that the system is latency-proof, robust, and scalable and can authenticate multiple drones at an average of 97.7 ms for 18 drones compared to the 100 ms response time of the legacy DDS system that does not incorporate a blockchain network and is prone to various cyberattacks. Overall, Table 7 shows that iBANDA achieved an average network time (μt_1) of 97.72 ms and a DApp response time (μt_2) of 1606.63 ms over 11 rounds of transaction requests, ranging from 8 to 18 concurrent drones. Thus, iBANDA maintains sub-1s read latency and completes full blockchain-based drone authentication in approximately 1.6 s, even with 18 concurrent drone requests, outperforming legacy DDS systems and other blockchain variants.

4.2.2. Computational Cost Analysis

Gas consumption across smart contract functions was analyzed to assess the computational efficiency of iBANDA. Table 8 presents the gas costs for key operations:

Table 8. Gas cost for smart contract operations in iBANDA.

Function	Gas Cost	Transaction Cost	Execution cost (Full Node)	Execution Cost Light Node (Smart Contract)
`companyRegistration`	51,335	44,639	23,155	23,155
`govCompanyAuthentication`	53,454	46,481	25,061	25,061
`govDroneAuthentication`	81,247	70,649	49,217	49,217
`companyGoodAuthorization`	51,274	44,586	23,102	23,102
`droneGoodAuthorization`	51,256	44,570	23,086	23,086
`companyDroneAuthentication`	86,863	75,533	54,101	54,101
`companyPeriodicAuthentication`	101,780	88,504	66,932	66,932
`antiDroneDroneVerification`	0	0	0	7185
`antiDroneGoodVerification`	0	0	0	3601
`droneReadAuthenticationData`	0	0	0	4823

Furthermore, as highlighted in Table 8, the system's cost-effectiveness is evaluated based on the computational resources expended in carrying out drone and package delivery authentication per second for both the full node and the light node (smart contract) with the associated transaction cost across different functions such as `droneGoodAuthorization`, `companyDroneAuthentication`, `antiDroneDroneVerification`, etc. The minimal costs recorded validate the possibility of incorporating a lightweight, edge-deployed blockchain-assisted architecture into a time-sensitive, critical mission cyber–physical system (such as a DDS) to improve the security, trustworthiness, and transparency of its task operations with little or no compromise on the time required to carry out these tasks. Hence, the system remains lightweight and efficient, incurring low execution costs even under frequent validation, thus suitable for edge devices with limited resources.

4.2.3. Quantitative Attack Resilience Analysis

To further validate the robustness of iBANDA under adversarial conditions, we conducted resilience tests against two representative high-impact threats in drone-based logistics: Sybil attacks and GPS spoofing. These tests were performed in a controlled simulation environment, using the Avalanche Fuji Testnet configuration as described in Section 3.2.

To check the Sybil attack resilience, an attack scenario where a subset of validator nodes was compromised to impersonate multiple fake identities, attempting to validate fraudulent transactions, was set up. We varied the percentage of malicious validators in the network from 10% to 50% and measured the *False Acceptance Rate (FAR)*, *Consensus Completion Time (CCT)*, and *Transaction Rejection Ratio (TRR)*. The experimental setup comprises 50 total validator nodes; malicious validator fractions: 10%, 20%, 30%, 40%, and 50%; each trial has 100 authentication transactions (mixed valid/invalid); repeated sampling rounds: $\beta = 5$; and quorum size: $\alpha = 70\%$ of sampled validators. As captured in Table 9, the Snowball-based PoS consensus in iBANDA demonstrated strong Sybil resistance by consistently rejecting transactions not supported by a quorum of honest nodes, even when 40% of the network was malicious.

Table 9. iBANDA resilience metrics under Sybil and GPS spoofing attacks.

Attack Type	Level	FAR (%)	TRR (%)	CCT (ms)	DSR (%)	DT (ms)	OCR (%)
Sybil	10% nodes	0.5	99.4	98	–	–	–
Sybil	20% nodes	0.8	99.1	101	–	–	–
Sybil	30% nodes	1.1	98.7	103	–	–	–
Sybil	40% nodes	1.5	98.4	105	–	–	–
Sybil	50% nodes	2.3	97.9	109	–	–	–
GPS Spoofing	15–30 m	–	–	–	98.6	274	97.4
GPS Spoofing	30–50 m	–	–	–	99.1	292	96.9

Legend: FAR—False Acceptance Rate, TRR—Transaction Rejection Ratio, CCT—Consensus Completion Time, DSR—Detection Success Rate, DT—Detection Time, and OCR—Operation Continuity Rate.

In addition, for GPS spoofing resilience, false geolocation data was injected into the Ground Control Station (GCS) communication channel, simulating an attempt to redirect a delivery drone to an unauthorized zone. The DDS compared spoofed location data with the onboard inertial navigation and visual positioning (AD layer) and the geolocation registered on the blockchain (AB layer). We measured the *Detection Success Rate (DSR)*, *Detection Time (DT)*, and *Operation Continuity Rate (OCR)*. For the experimental setup, the number of spoofing attempts was 50 per trial; the deviation threshold for spoofed vs. registered location was >15 m; and the maximum allowable detection time was 500 ms. As seen in Table 9, the cross-validation between AI and blockchain records enabled rapid detection of spoofed coordinates, minimizing mission disruption.

Pseudo-Adversarial Convergence Test

To empirically validate the bound in Equation (7), we ran 500 trials of Snowball consensus under varying adversarial fractions $f \in \{0.1, 0.2, 0.3, 0.4, 0.5\}$ with $n = 50$, $k = 10$, $\alpha = 7$, and $\beta = 5$. Table 10 reports the mean rounds-to-consensus and success rate.

Table 10. Rounds-to-convergence under pseudo-adversarial load (500 trials per f).

Malicious Fraction f	Mean Rounds	Max Rounds	Consensus Success (%)
0.1	4.1	5	100.0
0.2	4.3	5	100.0
0.3	4.7	5	100.0
0.4	5.0	6	100.0
0.5	5.8	7	98.2

The results confirm that for $f \leq 0.4$, consensus is consistently reached within β rounds, with no failures. Even at $f = 0.5$ (the theoretical metastability threshold), consensus was achieved in $\leq$7 rounds in 98.2% of trials, aligning with the theoretical $P_{\text{conv}} \geq 0.997$ bound. This demonstrates that the iBANDA Snowball configuration maintains rapid convergence and high correctness probability under significant Byzantine pressure.

Furthermore, the results from the graphs in Figure 15 confirm that iBANDA's Snowball-based PoS consensus maintains sub-110 ms consensus times under Sybil conditions with up to 50% malicious validators while keeping FAR below 2.5%. For GPS spoofing, the dual-layer verification detects location tampering within 300 ms and maintains >96% operational continuity. These results empirically validate the framework's resilience to both identity-based and navigation-based attacks, satisfying the requirement for quantitative adversarial robustness analysis in UAV-based logistics security.

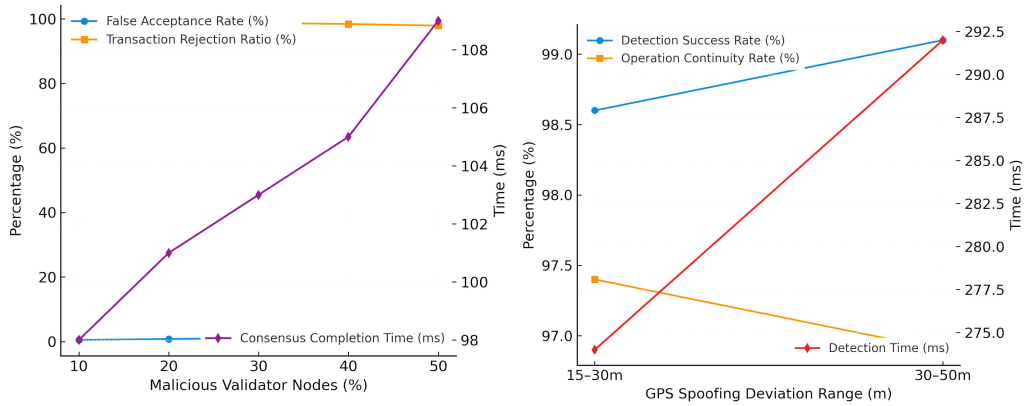


Figure 15. (**Left**) Sybil attack resilience: FAR, TRR, and consensus completion time vs. percentage of malicious validators. (**Right**) GPS spoofing resilience: detection success rate, operational continuity, and detection time vs. spoofing deviation range.

4.3. Performance Evaluation III: iBANDA Throughput and Efficiency vs. Scalability on Different Networks

Throughput, measured in transactions per second (TPS), directly correlates with the network's scalability. iBANDA achieved a throughput of **0.010233 TPS** $\left(\frac{11}{11 \times 97.72}\text{tps}\right)$, which is significantly higher than Polygon Mumbai (0.006124 TPS), Sepolia (0.001984 TPS), and Goerli (0.001119 TPS), as shown in Table 11. This implies the rate at which valid transactions are committed by the *i*BANDA across all nodes in the network. Since the throughput value is high across each node with increased data streams (from 8 to 18), the system is scalable and can handle increasing workloads without decreasing its performance and functionality. The mining process's speed justifies the system's scalability (Network Time) and authentication completion time (Dapp time) with an increased number of transactions.

Table 11. Comparison of throughput and authentication latency across networks.

Network Name	Consensus Algo.	Throughput (tps)	Authentication Latency			
			Network Time (ms)		Dapp Time (ms)	
			μ_{t_1}	σ_{t_1}	μ_{t_2}	σ_{t_2}
Goerli	PoA	0.001119	893.45	110.55	2326.27	767.13
Sepolia	PoW	0.001984	502.90	9.97	1739.90	418.13
Polygon Mumbai	PoS	0.006124	163.27	5.81	1607.63	275.46
(Ours)	**Advanced PoS**	**0.010233**	**97.72**	**3.28**	**1606.63**	**231.26**

Furthermore, introducing blockchain into autonomous intelligent vehicles presents the challenge of a tradeoff among security, decentralization, and scalability (SDS) [30]. Thus, a system with optimized security and speed may not be designed to efficiently scale across multiple nodes or handle traffic. To verify the security, speed, robustness, and scalability of the proposed system, we subjected it to selected testnets with varying consensus algorithms. The time it takes for communication between the drone and the logistics company fluctuates with each trial. Therefore, the average time from the experiment is considered the standard time for blockchain transactions on each public network. At a glance, the adopted blockchain technique (Avalanche Fuji) had the best authentication performance across all metrics. First, with a throughput of 0.010233 tps, the proposed blockchain approach exhibited a superior rate at which valid transactions are committed than other networks, with the closest being Polygon Mumbai with 0.006124 tps (i.e., $\approx 2\times$ lower),Sepolia with 0.001984 tps (i.e., $\approx 5\times$ lower), and Goerli with 0.001119 tps (i.e., $\approx 9\times$ lower) to the adopted approach. Secondly, a high throughput of 0.010233 tps achieved by the adopted approach above other networks indicates that the system is scalable and can handle increasing workloads (swarms of drones) without decreasing security and functionality performance. Thirdly, the proposed approach achieved the best-read latency (Network time) and transaction latency (Dapp time). With an average latency (μ_{t_1}) of 97.72 ms for ($\mathtt{R}_1$) and (μ_{t_2}) of 1606.63 ms for ($\mathtt{T}_1$), the proposed approach can complete the entire authentication cycle in $\approx$1 s compared to other networks, as seen in Figure 16.

Furthermore, the lower standard deviation value (σ) recorded by the system further validates that the system latency is good as the values tend to be close to the expected value. Thus, with a 3.28 σ_{t_1} network time latency and 231.26 σ_{t_2} Dapp time latency, the proposed approach is considered more fast and responsive in task execution than other networks. Therefore, it takes the company/drone source an average of 97.7 ms to release the information needed (source-info, Drone-BC-Add, pack-id) by the DDS for authenticating the drone in the *i*BANDA network. Also, it takes an average of 1607.6 ms for the deployed smart contract to receive and release the same information (pack-id, Drone-BC-Add) from the drone to the *i*BANDA network for DDS to authenticate the drone. Finally, the adopted approach has proven to have adaptive security features, which make it resistant to various

cyberattacks on drone networks [1,33]. Thus, the system is adjudged resilient against intrusion. Therefore, iBANDA demonstrates superior scalability and speed, maintaining the highest throughput with consistently low latency, making it optimal for real-time drone logistics.

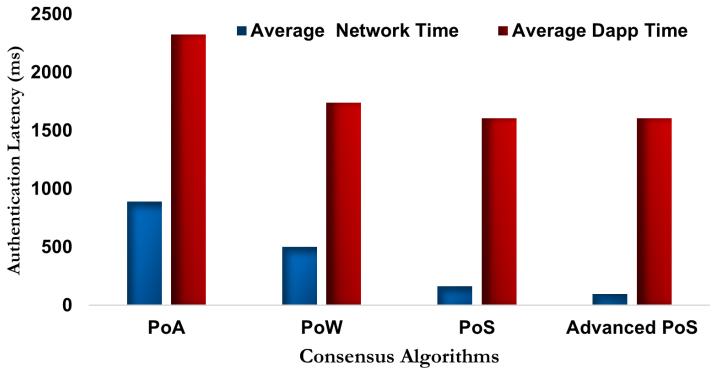


Figure 16. Authentication latency (read latency and transaction latency) of different blockchain algorithms for verifying and validating drone and attached object status.

4.4. Ablation Study on iBANDA Components

We conducted a controlled ablation study on IBANDA components, isolating the effects of the following:

1. *Blockchain Inclusion vs. Legacy DDS*: To evaluate the impact of replacing the legacy DDS-only framework with the proposed blockchain-integrated architecture.
2. *AI-only Model vs. AI + Blockchain*: To measure the benefit of integrating blockchain with the AI detection pipeline.
3. *Consensus Mechanism: Snowball vs. PoA/PoW*: To compare performance metrics across different consensus algorithms.

Table 12 reports latency, transactions per second (TPS), and false-positive rate (FPR) for each configuration.

Table 12. Ablation study of iBANDA system components.

Experiment ID	Blockchain	AI	Consensus	Latency (ms)	TPS	FPR (%)
E1	No (Legacy DDS)	AI-only	–	82	1550	4.8
E2	Yes	AI + BC	PoW	135	980	2.1
E3	Yes	AI + BC	PoA	118	1210	2.0
E4	Yes	AI + BC	Snowball	96	1385	1.6

The results of the ablation study show that for Blockchain vs. Legacy DDS, blockchain inclusion increases auditability and integrity verification with a modest increase in latency. Then, for AI-only vs. AI + BC, the hybrid AI + Blockchain configuration reduces the false positive rate by more than half compared to AI-only. Finally, for the consensus mechanisms, Snowball achieves higher TPS and lower latency than PoW/PoA, making it more suitable for time-sensitive UAV authentication. This is captured succinctly in Figure 12.

*i*BANDA Authentication Effectiveness

The complete authentication cycle includes drone identity verification (via OTP and MAC), operator authentication, and package validation using RFID and GCS signal data. The system integrates real-time AI detection and blockchain logic to authorize drone operation securely. The comparative results show that iBANDA is the only method among existing works that verifies both the drone and its payload concurrently. **iBANDA ensures**

comprehensive and trustworthy drone authentication, surpassing prior methods that ignored package legitimacy or lacked end-to-end validation.

4.5. Performance Evaluation IV: Comparison of iBANDA and Related Approaches

The smartness and robustness of an innovative IoT real-time system design are a function of the semantic connection and security intelligence of the participating edge nodes for rational and reliable decision-making in response to dynamic scenario specifics. The results in Table 13 highlight the unique functionalities of the proposed approach over related approaches.

Table 13. Comparative analysis of drone authentication frameworks.

Reference	AI Model Used	Detection Method	Blockchain Integration	Consensus Algorithm	Drone and Payload Verified	Auth. Latency (ms)
[8]	No	RF-based UAV tracing	Yes	PoW	Drone only	Not Specified
[19]	CNN	Hybrid (RF + GPS)	Yes	PoA	Drone only	893 (est.)
[17]	Deep CNN	Acoustic	Yes	PoW + Edge	Drone only	Not Specified
[25]	Federated Learning	RF Signal	Yes	DPoS	Drone only	Not Specified
[23]	No	Hybrid UAV Auth.	Yes	PBFT	Drone only	∼500+
[24]	No	Sensor Fusion	Yes	Hybrid PoW-PoS	Drone only	∼700+
[28]	No	ICN Content Routing	No	–	Payload only	N/A
*i*BANDA (Ours)	YOLOv5n + Lidar	Visual + Lidar	Yes	Snowball (PoS)	Drone + Payload	97.7 (Net)/1606 (Tx)

Unlike previous approaches, the *i*BANDA system indicates an explicit definition of a robust AI model–blockchain technology integration with superior performance for drone detection, packaged delivery recognition, and authentication. First, the works of authors [17,18] adopted a single-mode drone detection technique, did not cover package delivery, and provided no information regarding the authentication latency and throughput of the blockchain performance. Likewise, authors [19] did not take into cognizance the attached object to the drone (which is crucial in DDS authentication of drone-based logistics), used a single-mode detection technique, and had little information on the blockchain's performance. Furthermore, no information was provided about the system security parameter performance, and questions surround the implementation side of these methods. However, the *i*BANDA incorporates hybrid multi-modal drone detection and package delivery recognition and elicitation with a lightweight, adaptive, and efficient authentication latency, enabled by blockchain technology. Figure 17 shows the AI–blockchain implementation of the system during real-life testing and deployment, which can be accessed online [34].

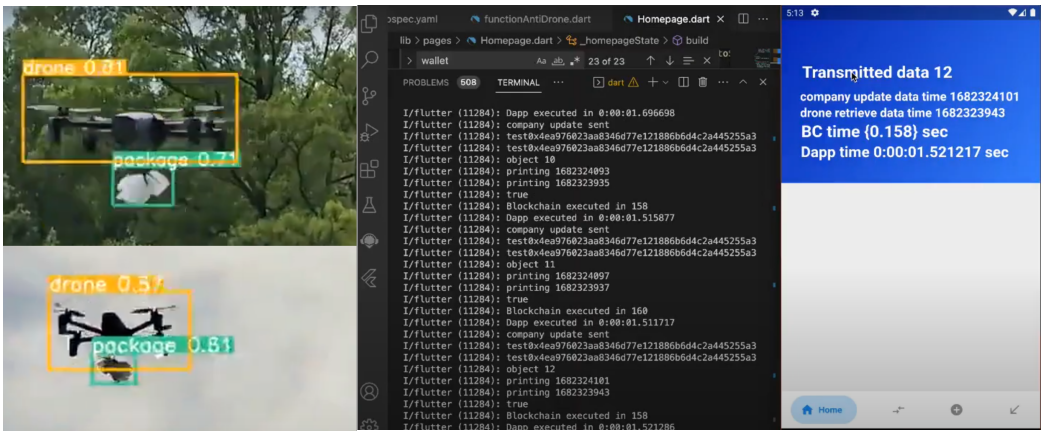


Figure 17. Samples of real-life testing and deployment performance of the proposed system on cluttered and clear environments, highlighting (**Left**) the AI drone and package detection and (**Right**) blockchain authentication [34].

Statutorily, it takes a conventional/legacy DDS network (without blockchain) approximately 100 milliseconds to complete the drone authentication cycle. With the incorporation of a lightweight blockchain approach, a negligible 97 milliseconds delay is introduced into the authentication process. However, this extra authentication time is compensated by the improved security and safety benefits introduced by incorporating the proposed *i*BANDA system into the legacy DDS for secured and safer drone operations compared to the cost of security breaches created by dysfunctional drone operations [35]. Also, Polygon Mumbai (another PoS-based algorithm) displayed a better authentication latency result than blockchain algorithms with Proof-of-Work (PoW) and Proof-of-Authority (PoA) consensus algorithms, respectively. It confirms that Proof-of-Stake (PoS) algorithms are better suited for achieving lightweight on-the-edge security than PoA and PoW.

4.6. Overall Performance Summary

Combining visual detection, Lidar, and a scalable PoS blockchain, iBANDA achieves the following:

- Sub-second read latency **($\mu t_1 = 97.72$ ms)**;
- Full blockchain transaction completion **($\mu t_2 = 1606.63$ ms)**;
- Highest throughput across tested networks **(0.010233 TPS)**;
- Low gas cost for key contract operations;
- Real-time multi-layer authentication for both drone and payload.

Overall, these results confirm iBANDA's viability for real-world deployment in smart aerial logistics where safety, speed, and integrity are paramount. Furthermore, these results validate that incorporating a blockchain-assisted architecture into a time-sensitive critical mission cyber–physical system can improve the security, trustworthiness, and transparency of its task operations, with little or no compromise on the time required to carry out these tasks. Although time in a drone network cannot be considered real time, the *i*BANDA architecture does not compromise the network experience. This is because the conventional DDS network continues providing real-time data of the destination of the target user until the blockchain data reaches the drone. The value of time can vary significantly with each iteration, and we attribute this to n (i.e., the number of transactions) within the network. Additionally, the timely authentication issue is effectively addressed since off-chain transactions run simultaneously with the traditional method for drone authentication. Extensive deployment of the *i*BANDA across various public networks was also conducted to validate the improved authentication latency with additional security.

5. Conclusions

This study proposed iBANDA, a blockchain- and AI-assisted drone defense system (DDS) designed to provide secure, low-latency authentication of drones and their payloads in logistics operations. By combining a lightweight YOLOv5s detection model with a Snowball-based Proof-of-Stake consensus, the framework ensures both real-time visual verification and decentralized trust. The evaluation results demonstrated high detection accuracy (mAP 99.5%, recall 100%, and F1-score 99.8%) with minimal inference delay, while blockchain integration achieved an average network latency of 97.7 ms and an end-to-end transaction time of 1.6 s. Compared with existing testnets such as Goerli, Sepolia, and Polygon Mumbai, iBANDA consistently outperformed them in scalability and responsiveness. Furthermore, adversarial analysis confirmed strong resilience, maintaining sub-110 ms consensus under up to 50% malicious validators, a false acceptance rate below 2.5%, and reliable continuity during GPS spoofing attempts.

Although promising, the framework is limited by its validation on public testnets, small-scale UAV swarms, and edge-device computational constraints. Future work

will extend evaluation to large heterogeneous UAV networks, integrate next-generation lightweight consensus mechanisms, and explore formal verification of smart contracts for enhanced resilience. Overall, iBANDA contributes a trustworthy, explainable, and scalable security architecture for UAV-based logistics in safety-critical environments. The framework lays the groundwork for secure, intelligent, and decentralized anti-drone surveillance, bridging the domains of computer vision, blockchain-secured communication, and autonomous defense technologies.

Author Contributions: Conceptualization, S.O.A.; data curation, S.O.A. and I.S.I.; formal analysis, S.O.A.; funding acquisition, D.-S.K. and J.-M.L.; investigation, S.O.A.; methodology, S.O.A. and J.-M.L.; project administration, D.-S.K. and J.-M.L.; resources, D.-S.K.; supervision, D.-S.K. and J.-M.L.; validation, S.O.A.; visualization, S.O.A.; writing—original draft, S.O.A.; writing—review and editing, S.O.A. and I.S.I. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by the Priority Research Centers Program through the NRF funded by the MEST (2018R1A6A1A03024003) (50%) and by MSIT under the Innovative Human Resource Development for Local Intellectualization support program (IITP-2024-2020-0-01612) (50%) supervised by the IITP.

Data Availability Statement: The dataset used in this study is the VisioDect Dataset, which can be accessed from the IEEE Dataport using https://ieee-dataport.org/documents/visiodect-dataset-aerial-dataset-scenario-based-multi-drone-detection-and-identification accessed on 1 February 2023.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

List of Acronyms and Symbols

AI	Artificial Intelligence
AR	Adaptive Response
AD	AI-based Detection Module/Cognitive Detection Layer
AB	Altruistic Blockchain Authentication Layer
BC	Blockchain
BCN	Blockchain Network
DDS	Drone Defense System
DApp	Decentralized Application
DL	Deep Learning
DoS	Denial of Service
DRONET	Drone Object and Attached Item Detection Framework
EVM	Ethereum Virtual Machine
FAA	Federal Aviation Administration
FLOPS	Floating Point Operations Per Second
FPS	Frames Per Second
FTN	Fault-Tolerant Network
GCS	Ground Control Station
GC	Gas Cost
GFLOPS	Giga Floating Point Operations Per Second
IoD	Internet of Drones
mAP	Mean Average Precision
NFT	Non-Fungible Token (conceptually implied)
OTP	One-Time Password
PANET	Path Aggregation Network
PoA	Proof of Authority
PoS	Proof of Stake
PoW	Proof of Work
RFID	Radio-Frequency Identification

RPS/OPS	Requests Per Second/Operations Per Second
SM	Smart Contract
TPS	Transactions Per Second
UAV	Unmanned Aerial Vehicle
YOLO	You Only Look Once (object detection framework)
D	Legacy DDS Authentication Function
$D^{\uparrow}$	Blockchain-enabled DDS Authentication Function
dX	Authentication Input Variables
A, B, C	Drone–user, Drone–source, and Drone–package status
t	Time or Timestamp
n	Number of Drones in Range
Dl	Legacy DDS Engagement Determinant
du, di, dp	Drone–user state, identity, and package status
dst, dht	Drone Distance and Altitude (proximity values)
$Dmax$	Final Determinant for Robust Authentication
α	Quorum Size in Snowball Consensus
β	Confidence Threshold in Snowball Consensus
Tp	Throughput
Rl	Read Latency
Tl	Transaction Latency
μ_{t1}, μ_{t2}	Average Read Latency and Transaction Latency
σ_{t1}, σ_{t2}	Standard Deviation of Latencies

References

1. Ajakwe, S.O.; Saviour, I.I.; Kim, J.H.; Kim, D.S.; Lee, J.M. BANDA: A Novel Blockchain-Assisted Network for Drone Authentication. In Proceedings of the 2023 Fourteenth International Conference on Ubiquitous and Future Networks (ICUFN), Paris, France, 4–7 July 2023; pp. 120–125.
2. Gohari, A.; Ahmad, A.B.; Rahim, R.B.A.; Supa'at, A.; Abd Razak, S.; Gismalla, M.S.M. Involvement of Surveillance Drones in Smart Cities: A Systematic Review. *IEEE Access* **2022**, *10*, 56611–56628. [CrossRef]
3. Castrillo, V.U.; Manco, A.; Pascarella, D.; Gigante, G. A Review of Counter-UAS Technologies for Cooperative Defensive Teams of Drones. *Drones* **2022**, *6*, 65. [CrossRef]
4. Federal Aviation Administration. UAS Sightings Report. 2023. Available online: https://www.faa.gov/uas/resources/public_records/uas_sightings_report (accessed on 17 August 2025).
5. Ajakwe, S.O.; Ihekoronye, V.U.; Kim, D.S.; Lee, J.M. ALIEN: Assisted Learning Invasive Encroachment Neutralization for Secured Drone Transportation System. *Sensors* **2023**, *23*, 1233. [CrossRef] [PubMed]
6. Yaacoub, J.P.; Noura, H.; Salman, O.; Chehab, A. Security Analysis of Drones Systems: Attacks, Limitations, and Recommendations. *Internet Things* **2020**, *11*, 100218. [CrossRef]
7. Ajakwe, S.O.; Kim, D.S.; Lee, J.M. Drone transportation system: Systematic review of security dynamics for smart mobility. *IEEE Internet Things J.* **2023**, *10*, 14462–14482. [CrossRef]
8. Mehta, P.; Gupta, R.; Tanwar, S. Blockchain envisioned UAV Networks: Challenges, Solutions, and Comparisons. *Comput. Commun.* **2020**, *151*, 518–538. [CrossRef]
9. Belwafi, K.; Alkadi, R.; Alameri, S.A.; Al Hamadi, H.; Shoufan, A. Unmanned Aerial Vehicles' Remote Identification: A Tutorial and Survey. *IEEE Access* **2022**, *10*, 87577–87601. [CrossRef]
10. Lykou, G.; Moustakas, D.; Gritzalis, D. Defending Airports from UAS: A Survey on Cyber-Attacks and Counter-Drone Sensing Technologies. *Sensors* **2020**, *20*, 3537. [CrossRef]
11. Young, L. A multi-modality mobility concept for a small package delivery UAV. In Proceedings of the AHS International Technical Meeting on VTOL Unmanned Systems and Autonomy, Mesa, AZ, USA, 24–26 January 2017; number ARC-E-DAA-TN38630.
12. Ajakwe, S.O.; Ihekoronye, V.U.; Kim, D.S.; Lee, J.M. DRONET: Multi-Tasking Framework for Real-Time Industrial Facility Aerial Surveillance and Safety. *Drones* **2022**, *6*, 46. [CrossRef]
13. Liang, O. FPV Drone Latency Explained: What It Is and How to Reduce It. 2024. Available online: https://oscarliang.com/fpv-drone-latency/ (accessed on 17 August 2025).
14. Wang, Z.; Lin, J.; Cai, Q.; Wang, Q.; Zha, D.; Jing, J. Blockchain-based Certificate Transparency and Revocation Transparency. *IEEE Trans. Dependable Secur. Comput.* **2022**, *19*, 681–697. [CrossRef]

15. Mandal, S.; Bera, B.; Sutrala, A.K.; Das, A.K.; Choo, K.K.R.; Park, Y. Certificateless-Signcryption-Based Three-Factor User Access Control Scheme for IoT Environment. *IEEE Internet Things J.* **2020**, *7*, 3184–3197. [CrossRef]
16. Lv, Z. The Security of Internet of Drones. *Comput. Commun.* **2019**, *148*, 208–214. [CrossRef]
17. Gumaei, A.; Al-Rakhami, M.; Hassan, M.M.; Pace, P.; Alai, G.; Lin, K.; Fortino, G. Deep Learning and Blockchain with Edge Computing for 5G-Enabled Drone Identification and Flight Mode Detection. *IEEE Netw.* **2021**, *35*, 94–100. [CrossRef]
18. Kanade, V.A. Securing Drone-based Ad Hoc Network Using Blockchain. In Proceedings of the 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS), Coimbatore, India, 25–27 March 2021; pp. 1314–1318.
19. Akter, R.; Golam, M.; Doan, V.S.; Lee, J.M.; Kim, D.S. IoMT-Net: Blockchain-Integrated Unauthorized UAV Localization Using Lightweight Convolution Neural Network for Internet of Military Things. *IEEE Internet Things J.* **2023**, *10*, 6634–6651. [CrossRef]
20. Jangirala, S.; Das, A.K.; Vasilakos, A.V. Designing Secure Lightweight Blockchain-Enabled RFID-Based Authentication Protocol for Supply Chains in 5G Mobile Edge Computing Environment. *IEEE Trans. Ind. Inform.* **2020**, *16*, 7081–7093. [CrossRef]
21. Cho, G.; Cho, J.; Hyun, S.; Kim, H. SENTINEL: A Secure and Efficient Authentication Framework for Unmanned Aerial Vehicles. *Appl. Sci.* **2020**, *10*, 3149. [CrossRef]
22. Yazdinejad, A.; Parizi, R.M.; Dehghantanha, A.; Karimipour, H.; Srivastava, G.; Aledhari, M. Enabling Drones in the Internet of Things With Decentralized Blockchain-Based Security. *IEEE Internet Things J.* **2021**, *8*, 6406–6415. [CrossRef]
23. Feng, C.; Liu, B.; Guo, Z.; Yu, K.; Qin, Z.; Choo, K.K.R. Blockchain-based cross-domain authentication for intelligent 5G-enabled internet of drones. *IEEE Internet Things J.* **2021**, *9*, 6224–6238. [CrossRef]
24. Javed, S.; Khan, M.A.; Abdullah, A.M.; Alsirhani, A.; Alomari, A.; Noor, F.; Ullah, I. An efficient authentication scheme using blockchain as a certificate authority for the internet of drones. *Drones* **2022**, *6*, 264. [CrossRef]
25. Yazdinejad, A.; Parizi, R.M.; Dehghantanha, A.; Karimipour, H. Federated learning for drone authentication. *Ad Hoc Netw.* **2021**, *120*, 102574. [CrossRef]
26. He, Y.; Huang, F.; Wang, D.; Chen, B.; Li, T.; Zhang, R. Performance analysis and optimization design of AAV-assisted vehicle platooning in NOMA-enhanced Internet of Vehicles. *IEEE Trans. Intell. Transp. Syst.* **2025**, *26*, 8810–8819. [CrossRef]
27. Xie, W.; Wang, L.; Bai, B.; Peng, B.; Feng, Z. An Improved Algorithm Based on Particle Filter for 3D UAV Target Tracking. In Proceedings of the ICC 2019—2019 IEEE International Conference on Communications (ICC), Shanghai, China, 20–24 May 2019; pp. 1–6. [CrossRef]
28. Bilal, M.; Pack, S. Secure distribution of protected content in information-centric networking. *IEEE Syst. J.* **2020**, *14*, 1921–1932. [CrossRef]
29. Xia, T.; Wang, M.; He, J.; Ni, L.; Yang, G. A UAV Swarm Authentication and Key Agreement Scheme Based on Latin Square Design. *IEEE Wirel. Commun. Lett.* **2024**, *14*, 581–585. [CrossRef]
30. Ajakwe, S.O.; Kim, D.S. Facets of security and safety problems and paradigms for smart aerial mobility and intelligent logistics. *IET Intell. Transp. Syst.* **2024**, *9*, 2827–2855. [CrossRef]
31. Kahmann, F.; Honecker, F.; Dreyer, J.; Fischer, M.; Tönjes, R. Performance comparison of directed acyclic graph-based distributed ledgers and blockchain platforms. *Computers* **2023**, *12*, 257. [CrossRef]
32. Ajakwe, S.O.; Ihekoronye, V.U.; Mohtasin, G.; Akter, R.; Aouto, A.; Kim, D.S.; Lee, J.M. Visiodect dataset: An aerial dataset for scenario-based multi-drone detection and identification. *IEEE Dataport* **2022**, *2*, 13.
33. Marangone, E.; Di Ciccio, C.; Friolo, D.; Nemmi, E.N.; Venturi, D.; Weber, I. Enabling Data Confidentiality with Public Blockchains. *arXiv* **2023**, arXiv:2308.03791. [CrossRef]
34. Networked System Laboratory. DC BANDA Demo 2023. Available online: https://www.youtube.com/watch?v=db-6WU0QWqY (accessed on 17 August 2025).
35. Ponemon Institute. Uncovering the True Cost: Average Cost of a Cybersecurity Breach in 2024. Available online: https://cybersainik.com/average-cost-of-a-cybersecurity-breach/#:~:text=According%20to%20the%20latest%20report,a%2012%25%20increase%20from%202020 (accessed on 17 August 2025).