IET Intelligent Transport Systems

WILEY

The Institution of Engineering and Technology

ORIGINAL RESEARCH OPEN ACCESS

Multihop Intruder Node Detection Scheme (MINDS) for Secured Drones' FANET Communication

Simeon Okechukwu Ajakwe[1] | Kazeem Lawrence Olabisi[2] | Dong-Seong Kim[3]

[1]Information and Communication Technology Convergence Research Centre, Kumoh National Institute of Technology, Gumi, South Korea | [2]International Centre for Professional Development, Federal University of Agriculture, Abeokuta, Nigeria | [3]NSLab Co., Ltd, Kumoh National Institute of Technology, Gumi, South Korea

Correspondence: Dong-Seong Kim (dskim@kumoh.ac.kr)

Received: 5 February 2025 | **Revised:** 14 July 2025 | **Accepted:** 13 August 2025

Funding: This research was supported by the Priority Research Centers Program through the NRF funded by the MEST (2018R1A6A1A03024003) (30%) and this work was supported by the IITP (Institute of Information Coummunications Technology Planning Evaluation)-ITRC (Information Technology Research Center) grant funded by the Korea government (Ministry of Science and ICT) (IITP-2025-RS-2024-00438430, 30%). This work was supported by the Institute of Information & Communications Technology Planning & Evaluation (IITP)-Innovative Human Resource Development for Local Intellectualization program grant funded by the Korea government (MSIT) (IITP-2025-RS-2020-II201612, 40%).

ABSTRACT

Unmanned aerial vehicles (UAVs) are becoming integral to time-sensitive logistics and intelligent mobility systems due to their flexibility, low deployment cost, and real-time connectivity. However, their open and dynamic communication environment—typically organized as flying ad hoc networks (FANETs)—makes them highly vulnerable to a wide spectrum of cyber threats. To address this, we propose a novel multihop intrusion node detection scheme (MINDS) powered by an AI-driven ensemble learning model, X-CID, optimized for lightweight drone networks. The proposed system integrates a decentralized multi-hop architecture with intra- and inter-cluster communication validation, enabling real-time anomaly detection across the physical, communication, and architectural layers of UAV systems. To improve detection performance under resource constraints, feature selection is applied using the Pearson correlation coefficient (PCC), and model hyperparameters are fine-tuned using randomized search cross-validation. Trained and evaluated on three benchmark datasets (WSN-DS, NSL-KDD, CICIDS2017) covering 24 distinct attack types, X-CID outperforms traditional models in F1-score (up to 99.84%), accuracy (up to 99.70%), and achieves low false alarm rates with competitive latency. The proposed approach ensures robust, scalable, and energy-efficient security for autonomous drone communication, making it suitable for critical missions in logistics, disaster response, and aerial surveillance.

1 | Introduction

There is a growing need for intelligent, secure, and time-efficient learning techniques that can handle the dynamic nature of end-to-end communication in drone transportation networks for prioritized logistics [1, 2]. Drone-based logistics is a paradigm shift from conventional logistics towards achieving a sustainable, eco-friendly environment that is in tandem with the sustainable development goals (SDG) as approved by the United Nations (UN), which is peace (SDGs 10, 16) [3, 4]. Therefore, a sustainable and resilient approach to drone networking to enhance drone mobility and logistics systems with 360-degree technological coverage [5] becomes imperative in achieving SDGs 10 and 16. However, increased communication mobility also heightens the risk of intrusion from unknown sources. Common cyber-attacks in the Internet of Things (IoT) ecosystem include DoS (denial of service), DDoS (distributed denial of service), MitM (man in the middle), R2L (remote to local), U2R (user-to-root), and spoofing

attacks [6]. These attacks aim to disrupt network operations, including drone networks. Finding a tactical approach and an optimal model to manage this dynamic, multivariate network traffic in real time while being resource-efficient is a significant challenge. Ensemble learning (EL) offers a solution by combining multiple machine learning algorithms to minimize the error of individual models and achieve better prediction results [7]. This approach helps avoid overfitting by averaging the outcomes of individual learners and expanding the search space of each classifier, leading to improved data representation.

The security and integrity of communication in autonomous aerial vehicular networks rely on reliable data sources, proper authorization, effective end-to-end connectivity management, and resource allocation among network nodes [8]. Today, drone-based networks, also known as the "Internet of Drones" (IoD), are increasingly used for autonomous aerial communication due to the low cost, high mobility, miniaturization of components, and maneuverability of UAVs [9, 10]. Generally, drones use the flying ad hoc network (FANET), which is a subset of mobile ad hoc networks (MANETs), to achieve connected communication intelligence due to FANET's ever-evolving topology, which allows the building of a high-speed (above 720 km/h) and extensive communication ecosystem (terrestrial, aerial, and space networks [11]). However, this cooperative communication intelligence in drones (drone-to-drone, drone-to-GCS, etc.) enabled by FANET faces various security challenges because of the limited functional security of their components, such as sensors, hardware, software, and communication links [4, 12]. Specifically, intrusion/cyber-attacks on FANETs cut across UAV-component attacks, UAV communication layer attacks, and UAV-communication architecture attacks [13] which can be either active or passive [14] depending on the motive of the intruder on the network, physical or logical (data-driven) [11]. A broader spectrum of cyber invasions on drones can be established via a comprehensive analysis of the vulnerabilities in FANETs and addressing them through an intuitive security system's modeling and design.

Drones and their networks are vulnerable to cyber-attacks even during the authentication phase, and this is a critical threat vector in real-world UAV deployments. The authentication stage is a high-value target because it is the entry point into the network and typically where trust is first established [15]. Despite advancements in UAV network design, one of the most critical yet often overlooked phases in drone communication is the authentication stage, which remains highly susceptible to cyber threats such as spoofing, replay attacks, and MitM intrusions. During this phase, adversaries may impersonate legitimate drones, inject malicious credentials, or replay previously captured signals to gain unauthorized access to the network. These attacks pose severe risks in FANETs, where drones frequently join or leave clusters in real time.

To achieve confidentiality, integrity, and availability (CIA) in UAV FANET, several approaches have been proposed to improve the capacity of intrusion detection systems (IDS), ranging from traditional techniques to machine learning (ML) and other artificial intelligence (AI)-driven methods, as summarized in Table 1. Examples of AI-driven IDS include SVM-based IDS [23], ensemble learning-based IDS [16], DT-based IDS [12], autoencoder-based IDS [17], and LSTM-based IDS [24]. Additionally, traditional supervised ML algorithms such as ensemble random forest (RF), Gaussian naive Bayes (GNB), and logistic regression (LR) have demonstrated their capability to detect and predict both known and new attacks, including various forms of DoS, MiTM attacks, eavesdropping, and fake data injections targeting IoD networks [12, 25]. However, as attacks become more sophisticated and datasets more varied, the limitations of existing IDS models become apparent in meeting the resource-constrained characteristics of drones and their networks. Also, existing approaches are constrained to detecting a limited number of cyber-attacks on drones' FANET without comprehensive coverage of cyber-attacks on UAV component attacks, UAV communication layer attacks, and UAV-communication architecture attacks [4, 13] arising from the dynamic deployment landscape of drones. Thus, it is crucial to implement a robust yet resource-friendly approach that can prevent intrusions at all levels of drones' FANET and is capable of addressing the emerging complexities of inter- and intra-drone communication transmission due to increased autonomous connectivity in critical missions.

Although traditional model-based and observer-based intrusion detection approaches, such as Kalman filters [21], unknown input observers (UIOs) [22], and residual generation methods [26] have demonstrated effectiveness in anomaly detection for cyber-physical systems, they are not emphasized in this study. These techniques typically depend on precise mathematical modeling of system dynamics and are most effective in deterministic, structured environments. However, in the context of highly dynamic and decentralized FANETs, accurately modeling the behavior of multiple heterogeneous drones under varying mission and network conditions becomes highly impractical. Moreover, these methods often lack scalability and adaptability in real-time, multivariate intrusion scenarios typical of UAV networks. This work instead focuses on scalable, data-driven, and learning-based techniques, which are better suited for resource-constrained drones operating in complex and rapidly changing environments.

In addition to data-driven and ensemble-based intrusion detection techniques explored in this work, prior research has also considered model-based and observer-based approaches such as Kalman filters [21], sliding mode observers [27], and UIOs [22]. These techniques rely on accurate system modeling and residual generation to detect anomalies in sensor data or actuator behavior. While effective in structured cyber-physical systems like SCADA, avionics, and industrial control, their applicability to dynamic, decentralized drone networks (FANETs) is constrained. The highly mobile and rapidly changing nature of UAV swarms complicates the derivation of accurate models, and these approaches often struggle with environmental noise, model uncertainties, and limited scalability. In contrast, machine learning methods, including decision trees, random forests, LSTMs, and autoencoders, offer greater adaptability and robustness in the face of complex, multivariate network traffic patterns [15]. The proposed X-CID framework builds upon this trend by delivering real-time detection and explainability, optimized for deployment on resource-limited UAV platforms. However, future research may benefit from hybrid models that combine model-based observers with learning-based techniques to enhance detection fidelity, interpretability, and resilience in UAV-based cyber-physical systems.

TABLE 1 | Comparative analysis of related works and the proposed approach.

Reference/method	Key Features	Limitations	Gap addressed by MINDS/X-CID
Autoencoder-based IDS [16]	Unsupervised learning for anomaly detection on NSL-KDD	No latency reported; lacks multiclass support; not optimized for UAVs	X-CID supports multiclass, latency-aware detection, optimized for UAV resource constraints
LSTM-based IDS [17]	Deep learning model trained on NSL-KDD and WSN-DS; suitable for time-series data	No time/error metrics reported; high complexity unsuitable for lightweight drones	X-CID uses low-complexity ensemble learning with better latency and performance
Random forest-based IDS [18]	High accuracy (CICIDS); interpretable model	Incomplete metric reporting; no multiclass or latency analysis	X-CID achieves complete evaluation (F1, latency, error), including multiclass attacks
Traditional ML models (RF, DT, GNB, LR) [19, 20]	Easy to implement, fast training	Poor generalization to diverse attack types; limited scalability in FANETs	X-CID enhances performance with feature selection, multi-dataset learning, and cooperative detection
Model-based/observer-based IDS [21, 22]	Uses Kalman filters, UIOs, residual analysis for cyber-physical systems	Requires exact system modeling; not scalable to dynamic drone networks	X-CID is data-driven and scalable for decentralized, real-time UAV environments
Proposed MINDS/X-CID	Ensemble-based, lightweight, explainable IDS with SCF, adaptive TTL, PCC, RandomSearchCV	Currently lacks integrated zero-trust authentication	Fills the gap in resource-efficient, delay-tolerant, scalable IDS for UAV FANETs with full-stack defense (component, communication, architecture layers)

Therefore, this work proposes MIND, a multi-connected, intelligent, secure, and comprehensive drone communication via an ensemble learning (EL) approach to detect cyber-attacks at all levels of the FANETs: physical component, communication layer, and communication architecture. This is aimed at improving reliable intra- and inter-communication feedback during drone operations and guaranteeing quality of service (QoS). It features an efficient and lightweight IDS (X-CID) that can rapidly and accurately detect malicious intrusions while ensuring ultra-fast connectivity. Furthermore, it advocates equipping the ground control station (GCS) and drone backbones with a robust and resource-friendly anomaly-based IDS framework (X-CID) that is empowered with a tiny ML prototype that possibly runs with a minimal power consumption of ≤10 mWs by choosing the best model with minimal computational complexity via the EL. Also, the approach enables nodes to intelligently defend against 24 well-known cyber-attacks that threaten the drone network's communication links. To ensure an effective model design, the randomized search cross-validation (RandomSearchCV) optimization technique was employed to fine-tune the hyperparameters of the selected random forest (RF) model. Key features of the dataset were selected using the Pearson correlation coefficient (PCC) technique to enhance detection speed and simplify the model. Considering that the IoD functions as a delay-tolerant network (DTN), the study emphasizes enhancing the network's resilience for swift attack detection while preserving the CIA of networked data.

This manuscript introduces a technically sound, novel, and context-aware intrusion detection framework-MINDS (multi-intelligent node decision system), for FANET-based UAV operations. The following are the key contributions of this work:

1. **A Novel Lightweight and Adaptive X-CID Framework for UAV Intrusion Detection:** We propose X-CID, a context-aware IDS tailored for the resource-constrained environment of UAVs. It integrates a random forest-based classifier with adaptive feature selection to achieve high accuracy (up to 99.9%) while maintaining computational efficiency suitable for real-time inference onboard drones.
2. **Integration of Delay-Tolerant Network Behavior Using Store-Carry-Forward and Adaptive TTL:** The framework introduces a delay-resilient communication strategy that combines a *store-carry-forward (SCF)* mechanism with an *adaptive time-to-live (TTL)* values. This ensures critical data packets are intelligently retained and retried, mitigating the risk of information loss in high-latency drone networks.
3. **Deployment-Aware Multi-Node Validation with Opportunistic Multi-Hop Routing:** We design a decentralized cooperative validation mechanism, where drones verify intrusion predictions collaboratively before transmission to the GCS. The use of opportunistic routing ensures robust communication and enhances detection reliability, even in the presence of dynamic connectivity and adversarial threats.
4. **Comprehensive Multi-Dataset Evaluation Validated by Strong Statistical Metrics:** We evaluate X-CID and MINDS across three benchmark datasets (WSN-DS, NSL-KDD, and CICIDS2017) in both binary and multiclass classification settings. Our approach achieves F1-scores up to 99.9%, Cohen's Kappa above 98%, and minimal MSE, confirming its robustness and generalizability.

Overall, this work bridges the gap between academic intrusion detection models and practical drone deployment by integrating

delay tolerance, cooperative intelligence, and real-time interpretability. It offers an adaptable and deployable solution for autonomous systems, cyber-physical security, and secure drone communication. Although the proposed MINDS framework verifies drone authenticity before deployment and classifies out-of-cluster communication as suspicious, it does not explicitly secure the authentication process itself against such identity-based attacks. To enhance resilience, incorporating zero-trust access control, mutual authentication protocols, and blockchain-based identity management to provide tamper-proof verification and robust access control at the network perimeter is needed, which is outside the scope of this work.

The remainder of this work is as follows. Section 2 captures the discussion of the decentralized IoD network architecture. Section 3 hints at the proposed learning technique, while the experimental setup, result discussion, and conclusion are presented in Sections 4 and 5.

2 | Decentralized Multi-Hop Intrusion Node Detection for Drone Network

The decentralized multi-hop intrusion node detection (D-MIND) drone network refers to the design and functioning of the IDS in a drone communication network that does not rely on a single centralized authority for decision-making, even though components like the GCS and UAV backbones exist in the architecture. Instead of having one centralized IDS located only at the GCS, the intrusion detection responsibilities are distributed across multiple UAV backbones and drones for local anomaly detection via their own lightweight AI-IDS (X-CID). Thus, the GCS participates in decision-making but doesn't control everything alone.

In practice, an attacker can potentially steal or mimic drone characteristics such as unique identifiers, firmware behavior, or communication signatures to masquerade as a legitimate UAV and infiltrate a drone network. This attack class is commonly referred to as drone impersonation, spoofing, or masquerading attacks. The proposed D-MIND framework addresses this via (i) pre-authentication verification; (ii) anomaly-based IDS (X-CID); and multi-hop monitoring that checks consistently for the drone's behavioral divergence.

Unlike conventional drone communication designs, this study asserts that the authenticity of the participating homogeneous drones is verified during the authentication phase before network setup and drone deployment. This pre-authentication verification ensures that only verified drones in the authentication phase are allowed into the network cluster. This is further validated by the short-range intra-cluster communication between the drones (D-2-D) enabled by the direct communication of each drone in each cluster with the UAV backbone, as well as inter-cluster communications between the UAV backbones. The anomaly-based IDS (X-CID) detects behavioral deviations, even from authenticated nodes, and monitors traffic consistency across intra-cluster and inter-cluster communications. Hence, out-of-cluster communication is treated as a malicious intrusion until proven otherwise. Furthermore, the multi-hop communication design ensures that drones communicate with backbone nodes, which filter and compare drone data using a heuristic database. When a drone's behavior diverges (e.g., a,$1 \neq$ a, $1'$), it is flagged and removed from the network. Therefore, if the impersonator behaves abnormally (e.g., sends unusual traffic, changes position patterns, or injects malformed packets), X-CID can detect it, even if the attacker bypasses initial identity verification.

The comprehensive multi-hop wireless nodal communication design, shown in Figure 1, shows the direct connections between all participating drones and the GCS within the network via the UAV backbone. This connection is logically realized through the corresponding UAV backbone node. Each cluster of drones communicates with a designated UAV backbone node, which acts as the cluster head and maintains a direct, secure link to the GCS. During mission-critical operations, the drones communicate in clusters (A, B, and C) with the GCS to optimize resource use and extend connectivity coverage over a long distance. Additionally, real-time telemetry data is transmitted periodically throughout the operations. Anomaly-based IDS using AI techniques is implemented on the UAV backbone to protect the network from malicious activities. The GCS and UAV backbone interaction is modeled as seen in Equations (1)–(3).

Given that:

$$U = \{u_1, u_2, u_3, \ldots, u_n\} \tag{1}$$

- U is the set of all UAV backbones in the drone network.
- Let ζ be the GCS signal.

Thus, the complete network graph is defined as;

$$G = (V, \forall) \tag{2}$$

where:

- $V = \{\zeta, u_1, u_2, u_3, \ldots, u_n\}$ includes the GCS and all backbone nodes,
- $\forall$ = denotes edges representing the direct communication links between the GCS and backbones and among backbones themselves.
- each u_i is connected to every other u_j such that $i \neq j$; where $u_i \leftrightarrow u_j$ connectivity is for UAV backbones and not individual drones.
- each u_i is directly connected to ζ as seen in Figure 1.

The adjacency matrix A in Equation (3) captures the topology of the UAV backbone network.

$$\therefore A_{i,j} = \begin{cases} 1, & \text{if connection between UAV backbones } i \text{ and } j \\ 0, & \text{otherwise.} \end{cases} \tag{3}$$

It represents the interconnections among the backbones and between each backbone u_i and the GCS ζ, capturing all connections to the GCS for inter-UAV backbone communications via the GCS authentic signal. $A_{i,j}$ models the routing and multi-hop communication paths; validates inter-backbone communication; and supports the cooperative intrusion detection mechanism in X-CID across backbones.

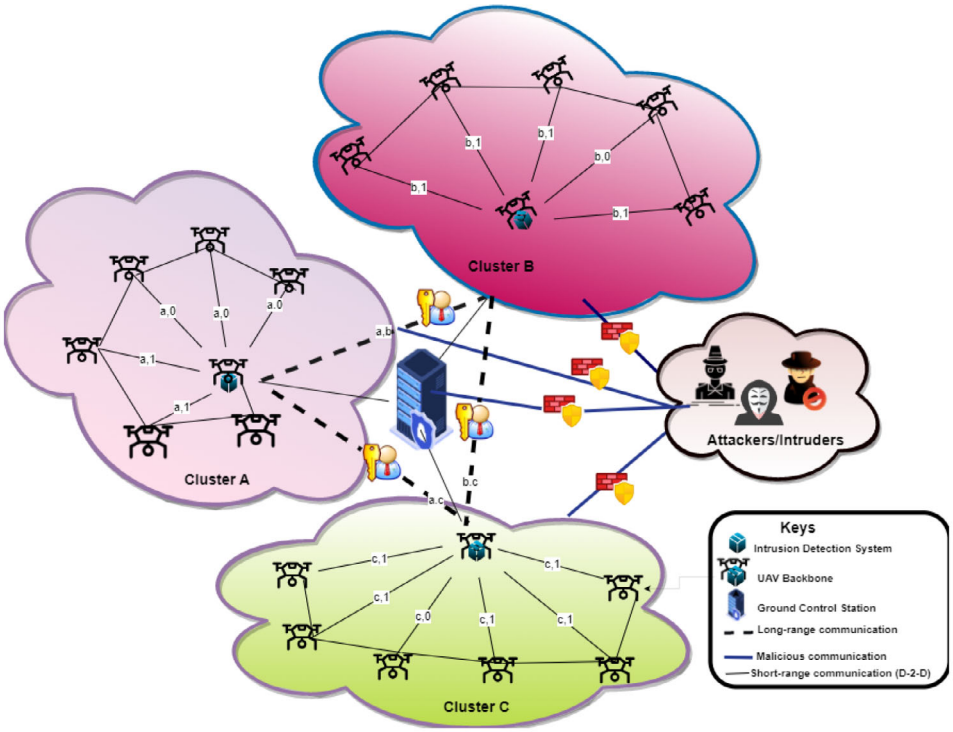

FIGURE 1 | Proposed MINDS framework for secured D-2-D communication.

Furthermore, to balance network resilience and security without incurring extra computational costs, the X-CID (see Section 3 for details) is integrated into the UAV backbones in each cluster (represented by the drone with the blue color "box-like" object) and the GCS for enhanced security. The proposed algorithm processes and models extensive normal and anomalous traffic data, automatically notifying the network of any deviation through attack detection and prediction. During flight operations, all data are transmitted to the UAV backbones in a multi-hop manner based on proximity before being sent to the GCS for final decision-making. Each UAV backbone (A, B, C) validates its cognitive information with that of the GCS. Thus, the UAV backbone acts as a cluster head, forming a hierarchical multi-hop routing architecture. Also, the UAV backbones interact with each other by intelligently sensing the correctness of the transmitted signal [(a, b), (b, c), (a, c)] from the GCS, respectively. With the authentic intercluster signal sharing among the UAV backbone, each UAV backbone joining the network and forming a new cluster can be reliably confirmed to extend the network coverage.

Then, each drone in the network interacts with drones within the same cluster (say, A) and communicates with the UAV backbone dedicated to that cluster as depicted in Equation (4).

Let $I(u_i, u_j)$ = interaction between drones in u_i and u_j. Then the GCS signal ζ, is defined $I(\zeta, u_i)$ as the interaction of ζ with u_i. Thus, the total system interaction S in each backbone and the entire GCS can be expressed as:

$$S = \sum_{i=1}^{n} \sum_{j=i+1}^{n} I(u_i, u_j) + \sum_{i=1}^{n} I(\zeta, u_i) \tag{4}$$

where:

- $\sum_{i=1}^{n} \sum_{j=i+1}^{n} I(u_i, u_j)$ is the interactions among drones in each cluster;
- $\sum_{i=1}^{n} I(\zeta, u_i)$ is the interactions of UAV backbones with the GCS (GCS-D communication).

In the event there is an attack/intrusion, as depicted with dark blue lines in Figure 1, the intelligent UAV backbones for each cluster monitor and manage the drone swarm, comparing and filtering traffic data for each UAV according to a heuristic database. When a node is compromised (say, a,$1 \neq$ a, $1'$), the UAV backbone responsible for the impacted cluster alerts the GCS, and the affected UAV is removed from the network. The routing table is then updated and broadcast. Likewise, suppose any of the UAV backbones are compromised. This can be anticipated in that case because there is direct communication between these backbones and the GCS, which is equipped with the proposed security model.

To safeguard the direct communication between each backbone and the GCS from tampering, secure alert transmission protocol (SATP) is incorporated for end-to-end encryption, as seen in Algorithm 1.

As shown in Algorithm 1, the SATP ensures authenticated and tamper-resistant communication between UAV backbones and the GCS With this inter-cluster and intra-cluster communication strategy, the MINDS ensures that at every given instance, the interaction of drones participating in the network is verified via security auditing based on the X-CID prediction.

Therefore, despite having GCS and backbones, the D-MINDS architecture is hierarchical in decision-making, with anomaly

ALGORITHM 1 | SATP between UAV Backbone and GCS.

Data: $\texttt{drone}_{\texttt{id}} = \texttt{d}$; $\texttt{threat}_{\texttt{type}} = \texttt{t}$; $\texttt{timestamp} = \texttt{T}$

Function GENERATE-ALERT (d, t, T)
  Alert ← (d, t, T, nonce) ← GenerateNonce()
end function

Function ENCRYPT-AUTHENTICATE (Alert, key)
  payload ← Serialize (Alert)
  mac ← HMAC (key, payload)
  encrypted ← AES_Encrypt(payload, key)
  return (data:encrypted, mac:mac)
end function

Function SEND-ALERT-TO-GCS (packet)
  Send packet to GCS
  Start acknowledgment time(T_{ack})
end function

FunctionON-GCS-RECEIVE(packet, key)
  decrypted ← AES_Decrypt(packet.data, key)
  if *HMAC*(key, decrypted) = packet.mac **then**
    Alert ← Deserialize(decrypted)
    if *IsFresh*(Alert.nonce, Alert.T) **then**
      Log AlertSEND-ACKNOWLEDGMENT(Alert.d, Alert.nonce)
      else
        Reject-packet(replay or stale alert)
      end
    end
    else
      Reject-packet (MAC verification failed)
    end
end
end function

Function ON-TIMEOUT
  if no acknowledgment received **then**
    Retry sending alert up to max retries
end
end function

Function SEND-ACKNOWLEDGMENT (d, nonce)
  ack ←{d, nonce, status : ACK, T : now()}
  Send ack to UAV Backbone
end function

ALGORITHM 2 | Enhanced MINDS Algorithm with Adaptive TTL.

Input :~Disaster Scene Data I, TTL base threshold T_0
Output:~Sensed and Validated Info (Sensor-info)
Initialize: prediction step $pr \leftarrow 4$, counter $i \leftarrow 0$;
Initialize: drones $D = \{d_1, d_2, ..., d_n\}$;
For each drone d_i:
  Capture data I;
  Assign priority $P \in$ {High, Medium, Low} to I;
  Set TTL value:
    if $P ==$ *High* **then**
      $TTL \leftarrow 3 \times T_0$;
end
    else if $P ==$ *Medium* **then**
      $TTL \leftarrow 2 \times T_0$;
end
    else
      $TTL \leftarrow T_0$;
end
while *true* **do**
  if *nearby drone* d_z *is available* **then**
    $d_i \rightarrow d_z$: transmit I;
    break
  else
    if *nearby GCS* g_j *is available* **then**
      $d_i \rightarrow g_j$: forward I;
      break
    else
      if *elapsed time* $T_s \geq TTL$ **then**
        Discard I from d_i buffer;;
        Log "TTL Expired: Data Discarded";
        break
      end
    end
  end
end
Function Sensor(data(d)):
  Initialize Sensor-info ← []
  foreach *feature* f_t *in data*(d) **do**
    if f_t*.isnan()* **then**
      $Nc_{f_t} \leftarrow$ calculate correlation using Equation (6);
      $r \leftarrow$ model.predict($[Nc_{f_1}, Nc_{f_2}, ...]$);
      Sensor-info.append(r);
    end
    else
      Sensor-info.append(f_t);
    end
end
return *Sensor-info*

detection happening at multiple levels for robustness: (i) within drone clusters (intra-cluster) via backbone node IDS; (ii) among backbones (inter-cluster) via mutual validation; and (iii) at the GCS through final verification. Even if one node or backbone is compromised, others can independently verify and respond, which is a key principle of decentralization in cyber defense. Thus, the D-MINDS ensures that an increase in the number of nodes does not translate to exposure to cyber-attacks via multiple security checkpoints using cooperative, layered defense mechanisms to guarantee resilient and secure drone operations even in adversarial environments.

3 | Ensemble Learning Intrusion Detection Framework

Figure 2 highlights the proposed exhaustive ensemble learning intrusion detection (X-CID) methodology, showing the various processes and stages for robust cyber-attack pattern recognition through feature engineering, prediction, and elicitation in a drone transportation network. The following subsection presents the steps undertaken to achieve the X-CID.

3.1 | Data Capturing and Communication Delay Handling

First, the drone that captures the information temporarily stores it in its buffer until a nearby node, such as neighboring drones or the backbone, becomes available. If communication delays exceed a certain threshold due to the limited bandwidth of the UAVs, the information may be discarded if no nearby node becomes available within the delay threshold, T_s (as seen in Algorithm 2 to preserve responsiveness). However, this can result in the loss of critical situational data needed for mission-critical operations.

To address this situation, we adopted a buffered redundant storage and priority tagging mechanism as shown in Algorithm 2. This mechanism employs a greedy buffering strategy (enhanced with adaptive time-to-live (TTL) values) to check the availability of nodes and authenticate communications between nodes of the network, ensuring that the network remains responsive to time-sensitive events and resilient to dynamic intrusions. Also, the multi-hop communication allows data to reach the GCS through intermediate drones or UAV backbones. The UAV backbone performs heuristic filtering and validation, enabling distributed decisions and avoiding overreliance on a single node or direct connection. As seen in Algorithm 3, adding store-carry-forward (SCF) techniques ensures that data is held and retried when feasible. This design improves resilience, delivery success, and efficiency under intermittent connectivity in drone networks.

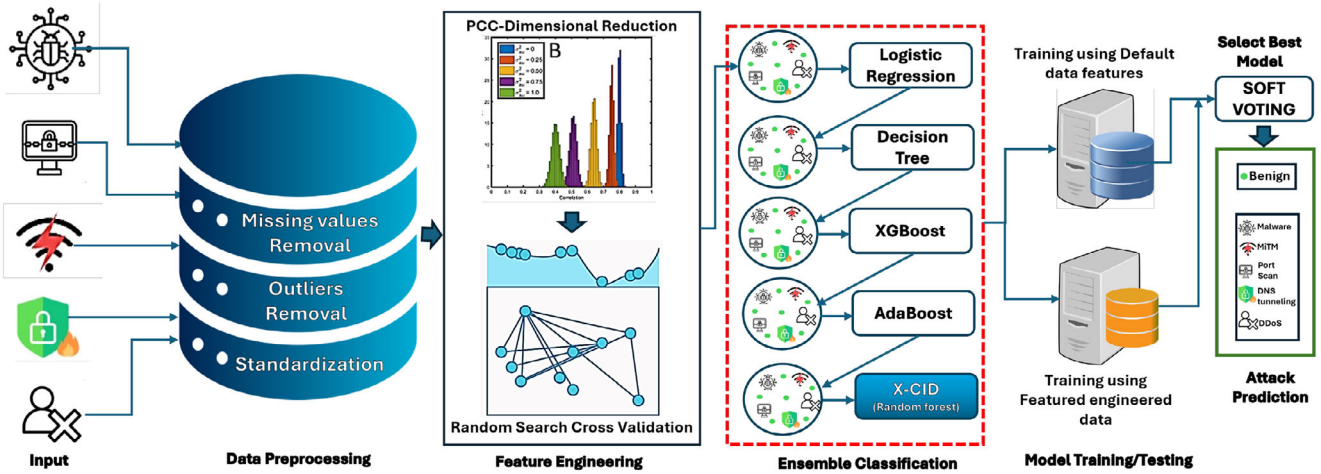

FIGURE 2 | Methodology for exhaustive cyber-attack intrusion detection (X-CID) in D-2-D and D-2-GCS communication.

ALGORITHM 3 | MINDS with Adaptive TTL and Store-Carry-Forward (SCF).

Input :~Captured data I, base TTL threshold T_0
Output:~Transmitted or Buffered Sensor-info
Initialize: prediction step $pr \leftarrow 4$, counter $i \leftarrow 0$;
Initialize: drone nodes $D = \{d_1, d_2, ..., d_n\}$;
For each drone d_i:
  Capture data packet I.
  Assign priority $P \in \{\text{High, Medium, Low}\}$.
  Set TTL:
    If $P ==$ High, $TTL \leftarrow 3 \times T_0$.
    Else if $P ==$ Medium, $TTL \leftarrow 2 \times T_0$.
    Else $TTL \leftarrow T_0$.
  Initialize buffer entry: $(I, TTL, T_s \leftarrow 0)$.
while $T_s < TTL$ **do**
  if *nearby drone* d_z *is available* **then**
    $d_i \rightarrow d_z$: transmit I;
    Log: "Data forwarded to neighbor drone";
    break
  else if *nearby GCS* g_j *is available* **then**
    $d_i \rightarrow g_j$: transmit I;
    Log: "Data forwarded to GCS";
    break
  else
    Store I in d_i's buffer for SCF retry;
    Increment elapsed time $T_s \leftarrow T_s + \Delta t$;
    Wait Δt and recheck neighbor availability;
  end
end
if $T_s \geq TTL$ **then**
  Discard I from buffer;
  Log: "TTL expired - Data discarded";
end
Function Sensor(data(d)):
  Initialize Sensor-info $\leftarrow$ []
  foreach *feature* f_t *in data*(d) **do**
  if f_t*.isnan()* **then**
    $Nc_{f_t} \leftarrow$ calculate correlation via Equation (6);
    $r \leftarrow$ model.predict($[Nc_{f_1}, Nc_{f_2}, ...]$);
    Sensor-info.append(r)
  else
    Sensor-info.append(f_t)
  end
end
return *Sensor-info*

As shown in Algorithm 3, the proposed SCF mechanism, combined with adaptive TTL values based on data priority, enhances responsiveness in delay-tolerant drone networks. High-priority data is assigned a longer TTL ($3 \times T_0$), and the drone periodically checks for available neighbors or GCS nodes before discarding data. However, under conditions of prolonged disconnection, such as in contested or infrastructure-denied environments, even high-priority packets may be discarded after TTL expiration. This could lead to the loss of critical information, rendering parts of the drone's mission ineffective if the lost data cannot be recovered or retransmitted. To address this limitation, future enhancements to the MINDS framework may include the use of multi-copy SCF routing, erasure coding, or mobile relay caching strategies. These would increase data survivability by ensuring that high-priority packets persist in the network until delivery becomes feasible. Additionally, incorporating drone-to-ground data drops or temporary local storage handoff to other drones could further mitigate the risk of mission-critical data loss.

3.2 | Dataset Preprocessing

Three (3) security-based datasets are used in this study to simulate and evaluate the models to avoid the accuracy paradox in model prediction. The accuracy paradox refers to a misleading situation in machine learning where a model shows high accuracy but performs poorly at the actual task, especially on imbalanced datasets [28, 29]. This can be prevented by using multiple datasets with different features, balancing the dataset, cost-sensitive learning, ensemble learning, feature engineering etc. [29]. Thus, we used the wireless sensor network (WSN-DS) dataset [30], the Canadian Institute of Cyber-Security Intrusion Detection (CICIDS2017) dataset [31], and the network security laboratory knowledge discovery data mining (NSL-KDD) dataset [32] to introduce diversity in feature space and attack patterns and helped models to generalize better, thereby avoiding biases towards one dataset's imbalance. Also, it reduces the risk of overfitting to one type of network or attack vector. The WSN-DS dataset comprises 4 DoS attacks with 23 features. Then, the CICIDS2017 dataset is a state-of-the-art dataset containing real-time network traffic and attack details with 83 features, 3,119,345 instances, and 15 attack types. Lastly, the NSL-KDD dataset is a legacy intrusion detection benchmark dataset with 125,973 and 22,544 instances and 5 attack types. Thus, 24 types of cyber-attacks common in drone networks are covered, cutting across attacks on the drone communication layer, architecture, and physical components [4].

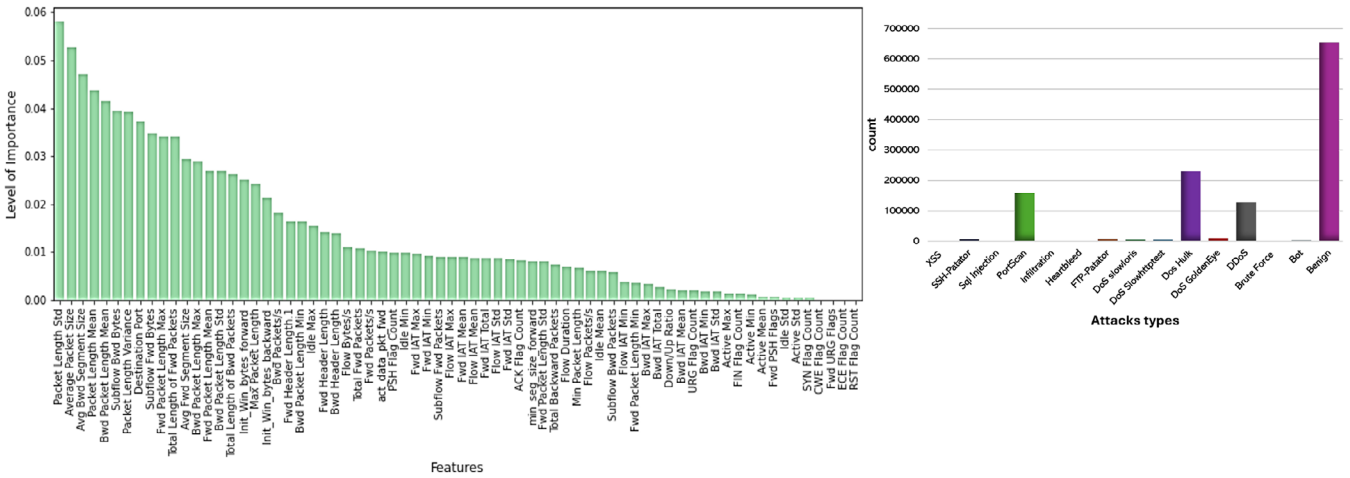

FIGURE 3 | CICIDS2017 dataset network traffic distribution before and after feature importance.

Second, when there is a disproportionate representation of classes in a dataset, a model is likely to predict the majority class's value for all predictions and achieve high classification accuracy, which is a biased outcome. To address these biases in the three datasets, missing values were expunged, outliers were removed, and standardization was carried out on the datasets to ensure that all values were on a similar scale and/or followed a particular distribution. Also, since the dataset did not follow a normal distribution and had positive values, a Box-Cox transformation [29] was carried out on the data as expressed in Equation (5).

$$Y(\lambda) = \begin{cases} \dfrac{Y^{\lambda} - 1}{\lambda}, \text{ if } \lambda \neq 0 \\ \log(Y), \text{ if } \lambda = 0 \end{cases} \tag{5}$$

where Y = original data point, and λ = transformation parameter. When $\lambda = 0$, the transformation is equivalent to the natural logarithm.

3.3 | Feature Engineering and Hyperparameter Optimization

After preprocessing, two feature engineering techniques, Pearson correlation coefficient (PCC) and random search cross-validation (Random SearchCV), were carried out on the datasets. The PCC selection strategy is applied to minimize computational complexity, reduce noise, enhance the interpretability of the predictive ML model, and boost the model's performance in terms of speed and accuracy. This is achieved by using the formula in Equation (6) to eliminate redundant features.

$$\Rightarrow \mathrm{R} = \left[\frac{\mathrm{N}\sum(\mathrm{xy}) - (\sum \mathrm{x})(\sum \mathrm{y})}{\sqrt{[\mathrm{N}\sum \mathrm{x}^2 - \sum(\mathrm{x})^2][\mathrm{N}\sum \mathrm{y}^2 - \sum(\mathrm{y})^2]}} \right], \tag{6}$$

where N = number of data points in the data set, $\sum xy$ = sum of the products of paired scores, $\sum x$ = sum of x scores, $\sum y$ = sum of y scores, $\sum x^2$ = sum of squared x scores, $\sum y^2$ = sum of squared y scores. In the end, the important features of each dataset are retained. Figure 3 highlights the distribution of the multiclass CICIDS 2017 dataset before and after the feature importance technique has been carried out on the dataset, indicating a significant improvement in the proportion of the normal class (benign with 654771) compared to the attack class (14 classes totalling 556,556). Figure 3 indicates that the attacks include `sql injection`, `DDoS`, `Bot` (for UAV components attacks), `DoS slowloris`, `DoS Slowhttptest`, `DoS Hulk` (for UAV communication attacks), and `PortScan`, `SSH Patator`, `FTP – Patator` (for UAV communication layer attacks).

To optimize hyperparameter selection while improving execution time, the adopted random search cross-validation approach identifies a bound domain of hyperparameter values and randomly samples points within that domain, fitting and scoring each estimator or model. Following this, a stratified 5-fold cross-validation is conducted to ensure that the optimized model maintains consistent and optimal detection performance, even when applied to unseen datasets. The specific set of hyperparameters used to construct the exhaustive ensemble learning model is detailed in Table 3.

The adopted RandomSearchCV process is summarized in Equation (7).

$$\theta^* = \mathrm{argmin}_{\theta_i \sim \Theta} \frac{1}{k} \sum_{j=1}^{k} L(M_{\theta_i}, D_{val}^{j}) \tag{7}$$

where:

- Θ = hyperparameter search space
- k = Number of folds in cross-validation (i.e., five-folds).
- L = Loss or performance metric function
- M_{θ_i} = model trained with hyperparameters θ_i.

The decision to use the RandomSearchCV technique is primarily driven by the minimal execution time it requires to select optimal hyperparameters, especially when compared to alternative methods. Also, the largeness of the parameter space of the selected datasets made it imperative to use RandomSearchCV as opposed to the GridSearchCV method. This makes it ideal for

TABLE 2 | Acronyms used and their meaning.

Acronym	Meaning
AI	Artificial intelligence
CIA	Confidentiality, integrity, availability
CICIDS	Canadian Institute of Cyber-Security Intrusion Detection
DL	Deep learning
DTN	Delay tolerant network
DT	Decision tree
EL	Ensemble learning
FANET	Flying adhoc network
GCS	Ground control station
GNB	Gaussian naïve Bayes
GPS	Global positioning system
IDS	Intrusion detection system
IoD	Internet of drones
IoT	Internet of things
LR	Logistic regression
LSTM	Long short term memory
MINDS	Multihop intrusion node detection scheme
ML	Machine learning
NSL-KDD	Network Security Laboratory Knowledge Discovery Data Mining
PCC	Pearson correlation coefficient
RF	Random forest
SCF	Store-carry-forward
SDG	Sustainable development goal
TTL	Time-to-live
UAV	Unmanned aerial vehicles
UN	United Nations
WSN-DS	Wireless sensor network dataset
X-CID	Exhaustive connected intrusion detection

time-sensitive operations, where quick detection of cyber-attacks in a drone network is crucial.

3.4 | Ensemble Model Training and Classification

The proposed X-CID methodology utilizes five ensemble learners—random forest (RF), AdaBoost, Gaussian naïve Bayes (GNB), logistic regression (LR), and decision tree (DT)—on three selected IoT network traffic datasets. The boosting ensembling method was adopted as opposed to the bagging, such that the performance of the new model was influenced by the performance of the previously built models. This was achieved by combining multiple weak learners to form a strong learner through sequential and iterative training of models as depicted in Figure 2 and summarized in equation

$$\epsilon_t = \frac{\sum_{i=1}^{N} w_t(i).1[h_t(x_i) \neq y_i]}{\sum_{i=1}^{N} w_t(i)} \tag{8}$$

where $1[h_t(x_i) \neq y_i]$ = indicator function that corresponds to 1 provided that $h_t(x_i) \neq y_i$, else 0.

TABLE 3 | Hyper-parameters optimal values.

S/n	Parameter	Values
1.	n_estimator	100
2.	max_depth	50
3.	max_features	3
4.	Criterion	Gini
5.	min_samples_leaf	3
6.	min_samples_split	8

The dataset was split into 80% training sets and 20% test sets based on the Pareto principle. Each participating model was trained and tested using the default data features and the feature-engineered data to validate the effectiveness of the proposed approach to cyber-attack prediction. The performance of each participating model is evaluated in terms of accuracy, recall/sensitivity, F1-score, prediction error, AUC-ROC etc., and these metrics are compared.

3.5 | Best Model Selection via Soft Voting Mechanism

Subsequently, a soft voting classifier is applied, using the outputs of the five ensemble learners as inputs, as shown in Figure 2. The soft voting classifier also referred to as a meta classifier, combines the results from RF, GNB, AdaBoost, LR, and DT to determine the attack types. This approach is particularly useful when the different ensemble learners perform similarly well, as averaging their outputs helps to mitigate the weaknesses of individual models. Unlike the hard-voting method, which bases the final prediction on the majority vote, the soft-voting classifier incorporates additional information, taking into account the strengths and limitations of each learner's classification method. The average predictions from all classifiers are used to categorize the attacks into their respective classes, depending on the dataset. Finally, the results from the soft voting classifier are distributed across the UAV backbone and the GCS, as depicted in Algorithm 2.

As seen in Algorithm 3, the adaptive TTL is adjusted based on data priority: High ($3\times T_0$), Medium ($2\times T_0$), Low (T_0). Then, the SCF mechanism ensures that if no neighbor or GCS is available, the drone stores the data and retries periodically within the TTL window. The retry mechanism ensures that the drone rechecks node availability every Δt time interval before the TTL expires. Finally, the discard policy checks if the TTL expires and no transmission is possible; the data is dropped with a log.

TABLE 4 | Summary of prediction result across datasets.

Models attacks predictions performance															
		Multi-class prediction							*Binary class Prediction*						
Datasets	**Metrics/ models**	**T (s)**	**Acc. (%)**	**F1 (%)**	**Rc (%)**	**Pr (%)**	**MSE**	**K**	**T (s)**	**Acc. (%)**	**F1 (%)**	**Rc (%)**	**Pr (%)**	**MSE**	**K**
WSN-DS	LR	160.0	96.71	82.70	82.60	84.84	0.086	80.68	4.800	98.50	95.60	95.60	95.60	0.014	91.40
	DT	0.643	99.55	97.28	97.22	97.41	0.010	97.44	0.392	99.60	98.80	98.80	98.08	0.003	97.72
	GNB	0.291	95.35	73.76	84.53	75.18	0.170	76.26	0.153	97.40	98.10	98.10	89.30	0.025	86.28
	AdaBoost	113.0	98.10	87.80	82.13	94.32	0.042	88.57	22.90	99.20	97.20	97.20	98.20	0.007	95.48
	RF	47.55	99.60	99.60	99.60	99.60	0.009	97.71	44.32	99.69	99.69	99.69	99.69	0.0031	98.16
	X-CID	**29.00**	**99.64**	**97.70**	**97.94**	**97.57**	**0.008**	**97.95**	**32.40**	**99.70**	**99.84**	**99.84**	**99.84**	**0.002**	**98.24**
NSL KDD	LR	0.49	9119	85.79	83.39	89.36	0.74	97.52	0.623	95.1	95.1	95.0	95.1	0.018	98.40
	DT	0.09	97.13	92.15	91.33	93.13	0.16	97.11	0.459	96.0	95.0	96.0	96.1	0.009	98.19
	GNB	0.03	82.10	70.28	83.95	73.59	0.86	87.64	0.146	94.6	94.5	94.6	94.5	0.240	89.17
	AdaBoost	1.39	42.24	49.90	55.35	56.19	5.83	90.15	10.10	96.7	96.6	96.2	96.7	0.070	93.36
	RF	1.680	95.58	95.58	95.57	95.58	0.15	95.14	1.460	97.5	97.5	97.5	97.5	0.014	97.10
	X-CID	**0.749**	**97.24**	**96.38**	**95.93**	**96.54**	**0.13**	**96.51**	**4.510**	**99.4**	**99.4**	**99.7**	**99.1**	**0.006**	**98.59**
CICIDS 2017	LR	1573	95.2	67.99	63.8	75.5	1.47	80.68	135	90.4	90.4	90.8	90.5	0.095	91.40
	DT	14.2	99.7	99.4	98.2	98.6	0.07	97.44	14.5	99.7	99.7	99.7	99.7	0.002	97.72
	GNB	2.03	67.1	55.2	74.4	56.9	8.92	76.26	1.14	72.4	71.5	74.3	79.8	0.275	86.28
	AdaBoost	271	66.8	20.0	26.6	16.9	9.80	88.57	257	99.2	99.2	99.2	99.2	0.007	95.48
	RF	478.0	99.6	99.6	99.6	99.6	0.18	99.31	410.8	99.6	99.6	99.6	99.6	0.003	99.26
	X-CID	**181**	**99.8**	**99.1**	**98.8**	**99.3**	**0.04**	**97.95**	**198**	**99.9**	**99.9**	**99.9**	**99.9**	**0.001**	**98.24**

Each of these classifiers is recognized for effectively predicting network traffic, each with its own biases. However, RF is used as the baseline ML model for comparing the predictive performance of other classifiers due to its low complexity, fast prediction time, and robustness in handling imbalanced datasets. The proximity function between two features, k and l, can be defined using the RF voting mechanism. This depends on the correlation between the trees and their strength, represented by the proportion of trees in the RF model that classify both k and l into the same classes, as shown in Equation (9).

$$\Rightarrow \mathtt{prox}_{(k,l)} = \left[\frac{\sum_{y=1}^{n_{tree}} 1(h_y(k) \equiv h_y(l))}{n_{tree}} \right], \tag{9}$$

where h_y is the y^{th} tree in the forest and $h_y(k)$ denotes the predicted value for k. Therefore, $\mathtt{prox}_{(k,l)}$ corresponds to 1 if all the trees in the forest classify k and l in the same classes. RF models tend to overfit. To overcome this, hyperparameter optimization is carried out with a set of well-performing parameters for the optimal configuration of the model.

3.6 | Experimental and Simulation Setup

All the simulation experiments of the ML models are carried out in a Python environment with Tensorflow 2.9.0 and Keras library in Python environment on a Windows 10 operating system with the hardware configuration of Intel(R) Core(TM) i5-8500 CPU @ 3.00GHz, 6Core(s), NVIDIA GeForce GT 1030, GPU CUDA:0 (Tesla K80, 11441.1875MB), and 36GB RAM.

4 | Result Discussion and Performance Evaluation

To ensure a robust analysis of simulation results on the three datasets (WSN-DS, NSL KDD, and CICIDS 2017), each model's prediction is subjected to several performance evaluation metrics, such as training time (T), accuracy (Acc.), recall (Rc), precision (Pr), F1-score (F1), means squared error (MSE), and Cohen Kappa (K) as shown in Table 4. Cohen Kappa (K) measures the inter-reliability and intra-reliability for qualitative categorical items that are mutually exclusive. In classical ML, the value of K can be derived from a 2 by 2 confusion matrix, as highlighted in Equation (10).

$$K = \frac{2 * (T_p \times T_n - F_n \times F_p)}{(T_p + F_p) \times (F_p + T_n) + (T_p + F_n) \times (F_n + T_n)}, \tag{10}$$

where T_p = true positive; T_n = true negative; F_p = false positive; and F_n = false negative value. The following section presents a detailed discussion of the model's performance in predicting drone network-related cyber-attacks.

TABLE 5 | Comparison of the proposed technique with related works.

Attack prediction performance of state-of-the-art models						
Ref.	**Model**	**Dataset**	**Prec. (%)**	**F1-score (%)**	**Time (s)**	**Error (MSE)**
[16]	RF	CICIDS (Bin.)	99.9	99.9	—	—
[16]	RF	CICIDS (Multi.)	99.9	99.9	—	—
Ours	**X-CID**	CICIDS (Bin.)	**99.9**	**99.9**	**198**	**0.001**
Ours	**X-CID**	CICIDS (Multi)	99.8	**99.1**	**181**	**0.040**
[17]	Autoencoder	NSL	86.8	92.2	—	0.017
[24]	LSTM	NSL (Bin.)	85.0	90.0	—	—
[24]	LSTM	NSL (Multi)	80.0	88.0	—	—
Ours	**X-CID**	NSL (Bin.)	**99.4**	**99.4**	**4.51**	**0.006**
Ours	**X-CID**	NSL (Multi)	**97.2**	**96.5**	**0.75**	**0.130**
[24]	LSTM	WSN-DS (Bin.)	85.0	90.0	—	—
[24]	LSTM	WSN-DS (Multi)	90.0	90.0	—	—
Ours	**X-CID**	WSN-DS (Bin.)	**99.7**	**99.1**	**32.4**	**0.002**
Ours	**X-CID**	WSN-DS (Multi)	**99.6**	**97.5**	**29.0**	**0.008**

4.1 | Model Prediction of Intrusion on Drone Networks

This section evaluates the predictive performance of several machine learning models, focusing on the proposed X-CID framework and its baseline model—random forest (RF)—using three benchmark datasets: WSN-DS, NSL-KDD, and CICIDS2017. The evaluation covers both binary and multiclass classification tasks, and uses metrics including accuracy, recall, precision, F1-score, MSE, Cohen's Kappa (K), and prediction time (T), as summarized in Table 4.

First, on the **WSN-DS** dataset; in binary classification, the Random Forest (RF) model achieved an impressive F1-score of 99.60%, accuracy of 99.69%, minimal MSE of 0.0031, and Cohen's Kappa of 98.16, indicating excellent agreement between predicted and actual classes. With a low prediction time of 44.32s, RF demonstrated a favorable balance between precision and latency. However, the X-CID model outperformed RF, attaining an F1-score of 99.84%, accuracy of 99.70%, and a lower MSE of 0.002. Its Kappa value of 98.24 further confirms its reliability in distinguishing legitimate drone communications from anomalous behavior. In the multiclass setting, X-CID also maintained robust performance, achieving an F1-score of 97.70% and Kappa value of 97.95, albeit with slightly longer training time than the decision tree classifier.

Second, for the **NSL-KDD** dataset, which presents a broader spectrum of attack vectors, RF achieved a 97.52% F1-score, 97.50% accuracy, and an MSE of 0.014. These results validate RF's effectiveness even under imbalanced class distributions. X-CID, however, delivered superior results, with a 99.4% F1-score and accuracy, a remarkably low MSE of 0.006, and a high Kappa value of 98.59. The processing time of 4.51s demonstrates its suitability for real-time UAV-based detection tasks.

Thirdly, on this high-dimensional and realistic intrusion dataset (**CICIDS2017** dataset), the RF model continued to perform well, achieving a 99.6% F1-score, 99.6% accuracy, and MSE of 0.003. Nevertheless, X-CID achieved the highest performance across all metrics with a 99.9% F1-score, 99.9% accuracy, and near-zero MSE of 0.001 in binary classification. In the multiclass case, it reached an F1-score of 99.1% with a low error of 0.04 and Kappa value of 97.95, demonstrating strong predictive stability across diverse attack types.

Overall, across all datasets, RF consistently served as a strong baseline, demonstrating high classification accuracy and low error rates suitable for real-time drone environments. The X-CID framework, leveraging RF and additional enhancements, surpassed all benchmarks, especially in multiclass tasks and error minimization, while preserving fast inference times. These results validate X-CID's robustness for deployment in real-world FANET applications where intrusion detection must be both accurate and responsive.

4.2 | Performance Evaluation with Related Works

Additionally, to confirm the effectiveness and efficiency of the proposed technique, Table 5 provides a summary of the performance comparison with other state-of-the-art models deployed in the IoD network, all of which utilized the same datasets.

Based on the CICIDS2017 dataset, the comparative analysis from Table 5 shows that the RF model adopted by authors in [16] achieved the highest sensitivity (Prec.) of 99.9%. However, the authors did not include the values of other performance metrics, indicating a biased result. Also, the F1-score is a better metric than accuracy in ML because it guarantees the reliability of a model. Therefore, the proposed technique, with a sensitivity and F1-score of 99.9% each, a detection time of 198 s, and an error minimization

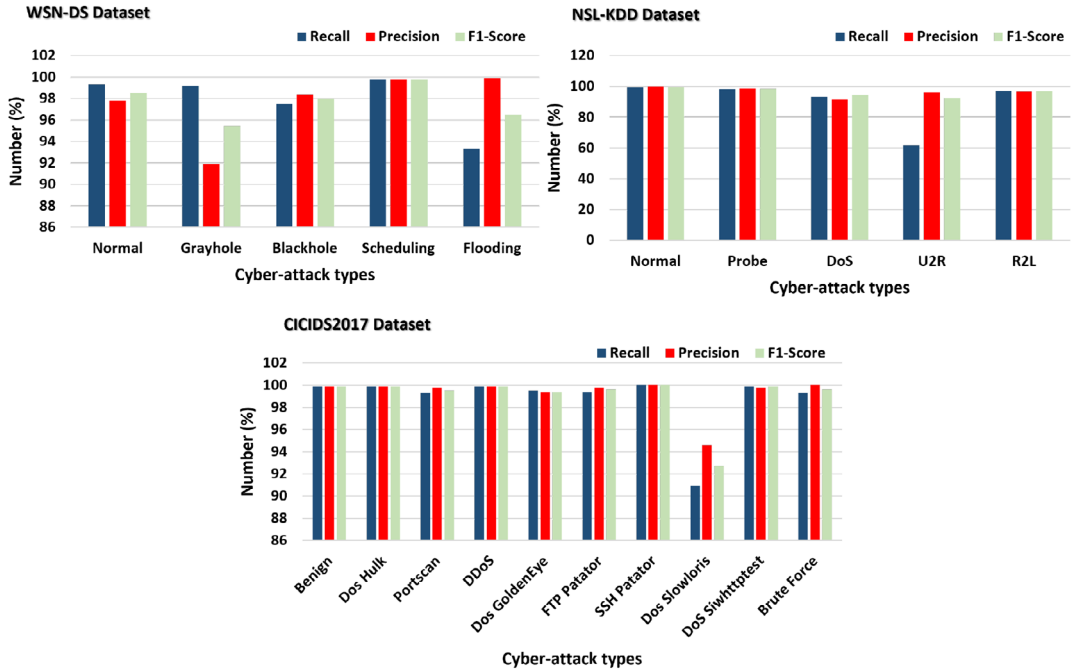

FIGURE 4 | Model robustness performance on the three datasets, highlighting the precision, sensitivity, and F1-score in predicting different types of cyber-attacks.

of 0.001, is better suited for validating the authenticity of drone network signals in binary classification. Likewise, for multiclass prediction, the proposed technique achieved better performance with a sensitivity of 99.8%, 99.1% F1-score, in 181 s, and a minimized prediction error of 0.040 compared to the RF model of [16], which did not consider time and prediction error, thereby casting doubt on its lightweight suitability.

Similarly, on the NSL-KDD dataset, the proposed technique delivered the best prediction results for both binary (99.4% precision, 99.4% F1-score, 4.51 s, 0.006 prediction error) and multiclass (96.5% precision, 96.3% F1-score, 0.75 s, 0.130 error) classifications across all metrics. This result is superior to those proposed by authors [17] and [24] using autoencoder and LSTM, respectively. Additionally, the authors [17] did not report the latency, while authors [24] did not report both latency and prediction error, indicating potentially inconsistent results.

Lastly, on the WSN-DS dataset, the proposed technique surpassed the works of authors [24] by delivering superior attack prediction performance for both binary and multiclass attacks. It excelled in sensitivity, F1-score, and latency, and prediction error, demonstrating its robust capability for effectively mitigating cyber-attacks on drone networks.

4.3 | Evaluation of Uniqueness of X-CID Technique

It is imperative to examine the performance of the X-CID in terms of its prediction robustness as the number and categories of cyber-attacks increase, its prediction capacity, and its efficiency for time-sensitive decision-making processes.

4.3.1 | Robustness

The results presented by the bar charts in Figure 4 summarize the performance robustness of the X-CID on WSN-DS, NSL-KDD, and CICIDS2017 datasets in terms of prediction sensitivity, rationality, and precision.

With a 99.8% F1-score value, 99.8% sensitivity, and 99.8% precision on the WSN-DS dataset, the X-CID can sufficiently curtail different forms of UAV-communication layer attacks on the drone network: grayhole, blackhole, scheduling, and flooding. This result implies that the proposed model (when adopted as the underlying predictive cognitive engine in UAV backbone and GCS) can adequately detect and help to prevent cyber-attacks on the network layer (`grayhole`, `blackhole`), physical layer (`scheduling`), and transport layer (`flooding`) targeted at the drones [4]. Thus, at any given instance of drone interaction, the proposed model if deployed in the drone backbone and GCS can decipher a genuine signal from different attacks targeted at the drone communication layer, as seen in Figure 4. Similarly, the X-CID achieved recall, precision, and F1-score values above 99% when detecting all the attacks in the NSL-KDD dataset except for a 61.5% recall value on U2R attacks. With a 99% F1 score in detecting }}`Probe`″, }}`DoS`″, }}`U2R`″, and }}`R2L`″ attacks, the proposed model can sufficiently detect the presence of dynamic abnormal signals (attacks) sent to any physical component of the drone network. This is seen by the 100% precision, recall, and F1-score values achieved by the X-CID in differentiating normal signals from attacks in the NSL-KDD dataset as highlighted in Figure 4. Lastly, the X-CID achieved a high detection and prediction of complex attacks at an average rate exceeding 95% in the CICIDS2017 dataset. Specifically, the results in Figure 4 indicate that the proposed X-CID with a 9.1% F1-score sufficiently detected most of the attacks on the

TABLE 6 | Scalability-enabling features in the MINDS framework.

Mechanism	Role in architecture	Scalability benefit
Hierarchical multi-hop communication	Organizes drones into clusters connected via UAV backbones	Reduces GCS load and allows easy network expansion
Decentralized anomaly detection (X-CID)	Enables local IDS on drones and backbones	Prevents performance degradation as node count increases
Opportunistic routing with Store-Carry-Forward	Ensures data delivery over unreliable links	Supports mobility and intermittent connectivity
Adjacency matrix $A_{i,j}$	Models inter-backbone connectivity	Supports dynamic cluster addition and routing updates
Feature selection via PCC	Reduces redundant input dimensions	Lowers computational load across all nodes

UAV components (DDos attacks), communication architecture (Dos Hulk, Dos Siwhttptest, Dos GoldenEye attacks), and communication layers (SSH Patator, FTP Patator, Portscan attacks) with the exception of Dos Slowloris with a 93% F1-score value. These results imply that the integration of the X-CID into the drone edge network will guarantee maximum security owing to its robust performance on different network intrusion datasets in detecting most FANETs' intrusions targeted at all the layers (network, physical, and transport), different drone components (hardware, software, and sensor), and the communication architecture (D-2-D, D-GCS) [4, 13]. Thus, the proposed model will ultimately help to guarantee robust inter- and intra-cluster communication and enhance safe drone mobility despite the increase in drone network cyber-attacks.

4.3.2 | Scalability

The scalability of the proposed MINDS is achieved through a combination of architectural and algorithmic innovations as captured in Table 6.

First, the network is organized into clusters, each managed by a UAV backbone node that serves as a local communication hub and intrusion detection point. These backbone nodes are directly connected to the ground control station (GCS) and also to one another, enabling both intra- and inter-cluster communication. This decentralized architecture prevents bottlenecks and allows seamless expansion as new drones and clusters are added. Furthermore, the proposed X-CID model is lightweight and optimized for deployment on resource-constrained UAVs. It enables distributed, real-time anomaly detection without overloading the GCS. The use of opportunistic multi-hop routing and a store-carry-forward mechanism with adaptive time-to-live values ensures data delivery even in the presence of intermittent connectivity, which is essential for mobile and large-scale deployments.

To formally model inter-backbone connectivity and support network growth, an adjacency matrix $A_{i,j}$ is defined, where each UAV backbone u_i maintains logical connections with other backbones u_j. This supports scalable routing and validation of drone behaviors across clusters. Additionally, feature selection via the PCC reduces computational complexity, allowing the IDS to maintain efficiency as the network scales. Collectively, these design choices ensure that the MINDS framework can support large-scale, delay-tolerant drone communication networks with minimal degradation in performance or security.

4.3.3 | Efficiency

The AUC-ROC curve in Figure 5 highlights the efficiency of the X-CID in distinguishing normal (benign) from anomalous data in the network. The receiver operating characteristics (ROC) as a probability curve that aids in the separation of 'signal' from 'noise' (errors) plots the true positive rate (TPR) against the false positive rate (FPR) at specific thresholds. On the other hand, the area under the curve (AUC) summarizes the ROC curve, as it is a measure by which the classifier can distinguish between normal and anomalous data. Therefore, a high AUC value indicates a good measure of separability by the model.

Generally, the perfect curve achieved by the X-CID in Figure 5 for both binary (AUC = 1.00) and multiclass classification (AUC $\approx$ 0.99) across the datasets indicates the high propensity of the X-CID for securing the drone network from all forms of lethal attacks at different classification thresholds. Specifically, on the CICICDS2017, the proposed approach achieved an AUC of 0.9997 in detecting most intrusions DoS Hulk, PortScan, DDoS, DoS GoldenEye, SSH – Patator etc., attesting to its efficiency in validating the authenticity of a communication signal in a drone FANET. Similarly, on the WSN-DS dataset, the proposed model achieved, on average, an AUC of 0.9975 in detecting and differentiating various attacks, grayhole, blackhole, scheduling etc., while maintaining a perfect curve of 1.00 AUC for binary classification. Finally, on the NSL-KDD dataset, the proposed model efficiently separates the drone signal from noise with an AUC value of 0.9834 for DoS, 0.9555 for Probe, 0.9710 for R2L, and 0.8712 for U2R attacks and maintains a perfect curve for binary classification. Consequently, these results imply that at any instance, the proposed model can efficiently decipher genuine drone communication signals from noise introduced into the network by intruders targeting any aspect of the drone network.

4.3.4 | Classification Capacity

The confusion matrices in Figure 6 highlight the classification capacity of the X-CID on intrusion prediction for both binary and multiclass data. For WSN-DS, a low false alarm rate of 0.10% was recorded, that is, an insignificant 795 packet misclassification compared to 241,958 correctly classified data. Similarly, the proposed model achieved a highly accurate classification rate of

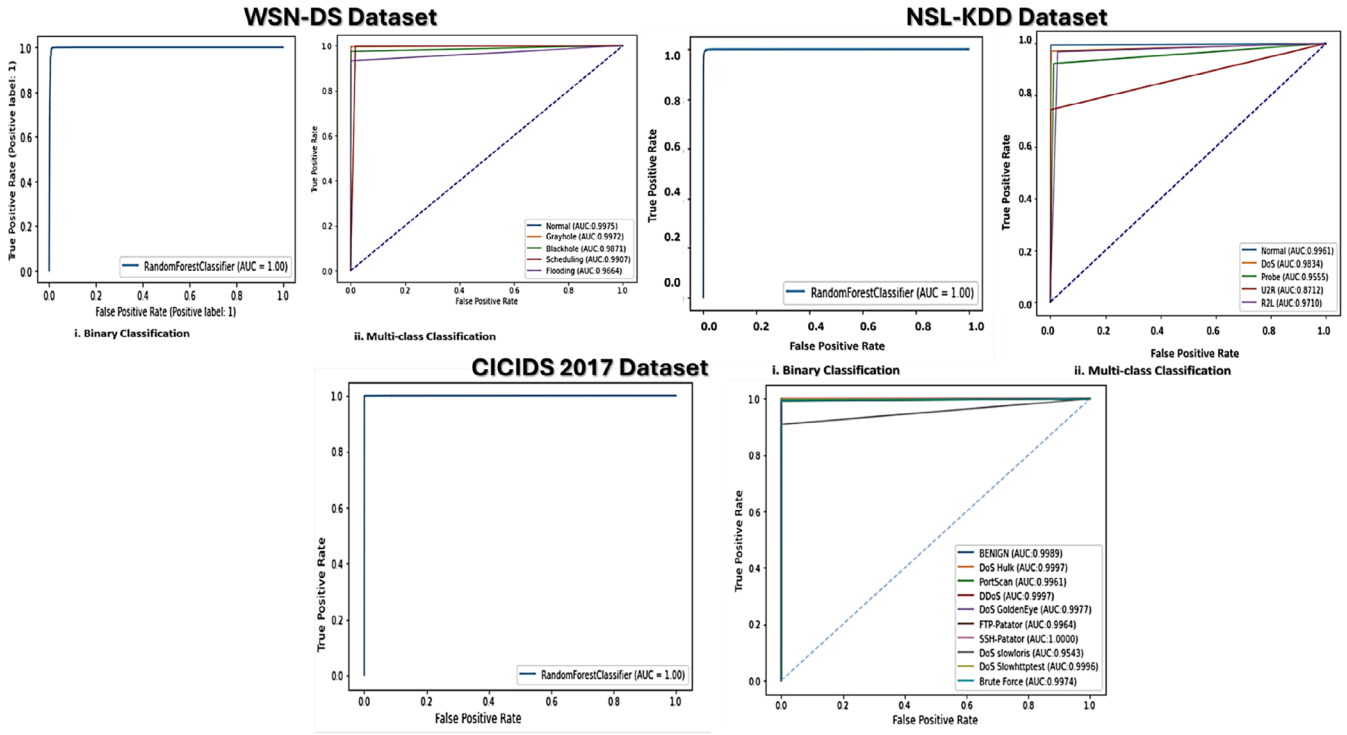

FIGURE 5 | Model cyber-attacks classification efficiency on the three datasets, indicating a near-perfect curve for binary and multiclass classification.

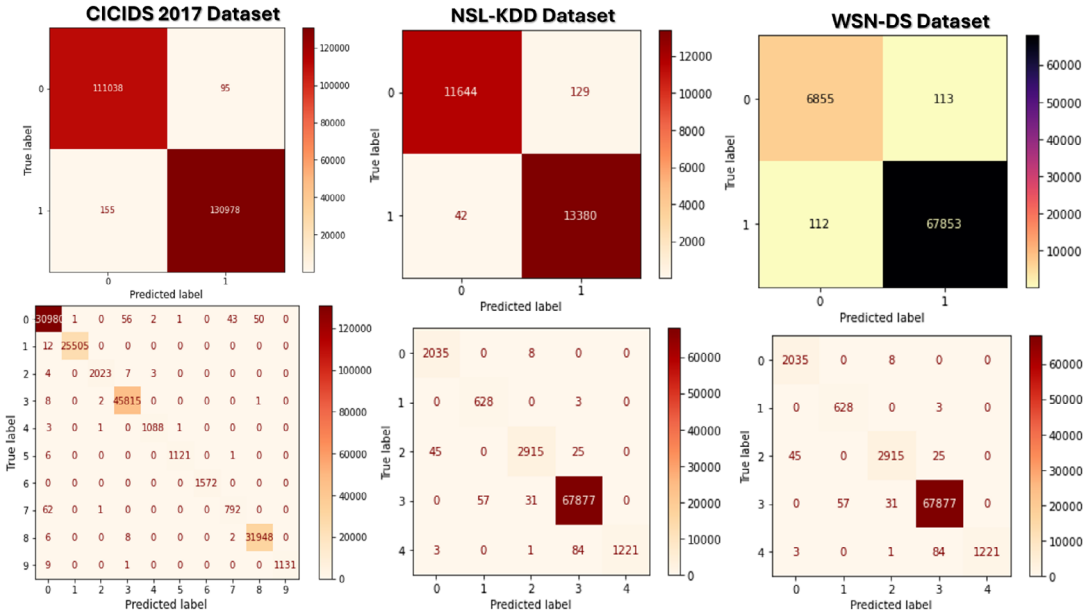

FIGURE 6 | Proposed model cyber-attack classification capacity on the three datasets for binary and multiclass classification, highlighting minimal misclassification of genuine and anormal signals.

11,644 true positive and 13,380 true negative values on the NSL-KDD dataset. Finally, in CICIDS2017 with diverse DoS attacks, the X-CID achieved a negligible 0.35% misclassification error, signifying high classification capacity to handle multivariate real-time network traffic. Conclusively, the minimal misclassifications on the three datasets (CICIDS2017, NSL-KDD, and WSN-DS) by the proposed model confirm the proposed approach's capacity to distinguish a genuine communication signal from a malicious signal in a FANET during communication: drone-to-drone, drone-to-drone backbone, or drone backbone to GCS. Thus, with an increase in traffic in the drone network, especially as the participating network node increases, the proposed model can, at any given instance, adequately handle and tackle intrusions targeted at either the drone, the drone backbone, or the GCS. Also,

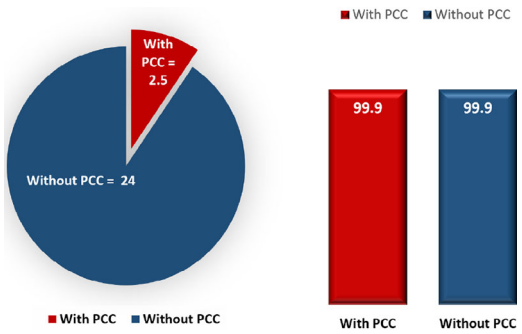

FIGURE 7 | PCC effectiveness on X-CID performance highlighting. (Left:) Time/latency. (Right:) Accuracy based on CICIDS2017 dataset.

with this classification capacity achieved by the proposed model as the underlying predictive cognitive engine in the drone backbones, safe and secure intra-cluster interaction between drones in the same cluster, inter-cluster interaction between drone backbones in different clusters, and drone-to-GCS interaction are guaranteed. Therefore, as the number of drones in the network increases, connected intelligence is maintained via the constant monitoring of the genuineness of drone communication carried out by the underlying X-CID model in the drone backbone. At any instance an intrusion is detected by the proposed model, it is immediately removed without jeopardizing the drone's mobility.

4.4 | Evaluation of PCC Optimization on X-CID

Figure 7 highlights the performance of the RF model before and after the proposed technique is applied to it.

Without the PCC, it took the model 24 min to detect intrusions, which is detrimental and time-consuming. However, with the application of the PCC, it took the model 2.5 min to execute the same task, indicating improved latency with a high accuracy of 99.9%. The results from these analyses prove that the proposed exhaustive ensemble intrusion detection (X-CID) technique is an adequate AI learning technique for achieving time-efficient, secure, and reliable intrusion detection in drone networks, irrespective of the network architecture, complexity of the dataset, and volatility of deployment terrain. Thus, improved latency is achieved via the incorporation of the PCC optimization on the X-CID, thereby resulting in timely intrusion detection and prediction, which is crucial in drone networks.

From the foregoing analysis, the X-CID has proven to be a resilient and resource-friendly AI-driven approach in mitigating cyber-attacks and intrusions in drone networks. With the X-CID as the underlying cognitive cyber-attack predictive model in the drone backbone and GCS, reliable drone intra-cluster and inter-cluster communication can be achieved for wider network coverage via multi-hopping connected intelligence. Undoubtedly, this will foster the deployment of safe and secure drones for long-range mobility and swarm tactical operations in developed and other emerging economies for military and other civilian purposes such as search and rescue operations, logistics, entertainment, mobile access points etc. However, not much is known about the human understanding of how the X-CID arrives at the attack prediction, thereby limiting the reliability of its logic. This is because the model's interpretability and explainability are still masked in a black box. Therefore, incorporating anthropomorphic characteristics into the X-CID, assisted by blockchain technology, will improve its logic's interpretability for maximum trustworthy security of the drone network.

While random search cross-validation and PCC are well-established methods in machine learning, their tailored application in the X-CID framework directly supports the model's ability to operate under UAV resource constraints. As demonstrated in Table 4, the X-CID consistently outperforms other models across all datasets in terms of F1-score, mean squared error (MSE), and detection latency. For instance, on the CICIDS2017 dataset, X-CID achieved a 99.9% F1-score and the lowest MSE (0.001) with a detection time of 198 s, significantly outperforming both classical and deep learning baselines. These results are made possible by the PCC's ability to reduce dimensionality and eliminate redundant features, improving both computational efficiency and detection accuracy. Likewise, RandomSearchCV accelerates hyperparameter optimization across a vast configuration space, enabling faster convergence compared to GridSearchCV. Together, these components contribute to the X-CID's lightweight yet robust performance. The latency improvement due to PCC alone is evidenced in Figure 7, where intrusion detection time was reduced from 24 min to 2.5 min without compromising accuracy. Therefore, although standard in isolation, the integration of these methods into a multi-level, distributed ensemble model optimized for drone FANETs makes their application novel, deployment-aware, and highly effective.

4.5 | Limitations and Future Directions

While the proposed MINDS framework, through its X-CID anomaly-based detection mechanism, effectively identifies malicious behavior within the drone communication network, it assumes that drones participating in the initial authentication phase are legitimate. However, in real-world scenarios, attackers may exploit vulnerabilities by spoofing or cloning legitimate drone identities—such as MAC addresses, firmware signatures, or communication patterns—to gain unauthorized access. These drone impersonation attacks pose a significant challenge, especially during initial cluster formation or mission deployment. Although X-CID can detect behavioral anomalies post-authentication, it does not inherently prevent identity-based infiltration at the network boundary. As part of future work, we propose integrating device-level fingerprinting, challenge-response authentication, and zero-trust access control into the authentication phase to enhance trustworthiness. Additionally, incorporating blockchain or distributed ledger technologies (DLTs) could offer tamper-proof identity verification and consensus-driven trust management, thereby preventing rogue UAVs from masquerading as legitimate nodes in the network.

Another limitation involves the risk of losing critical information if the drone cannot establish contact with any relay node before the TTL expires. Although priority tagging and retry mechanisms are implemented, prolonged disconnection can still cause data loss. Future versions of the framework may incorporate multi-copy SCF, fault-tolerant coding, or persistent relay drones to ensure guaranteed delivery of high-priority packets.

5 | Conclusion

This study developed a multi-hopping connected intelligence approach to drone networking and introduced an exhaustive learning technique, X-CID, aimed at optimizing AI-driven intrusion detection systems. This is to meet the growing need for secure drone transportation networks used in priority logistics, military tactical operations, and other critical time-sensitive missions. To enhance network resilience and resource efficiency while integrating speed, scalability, and improved cyber-attack prediction and prevention, the proposed model employed random search cross-validation and Pearson correlation coefficient methods to select optimal features on three public datasets and fine-tune the model's hyperparameters. This approach aligns with the lightweight nature of typical drone-based networks operating under resource constraints.

By testing the proposed model and other ML algorithms against three classic cybersecurity attacks and assessing their performance with various metrics, the study concludes that X-CID is a highly suitable framework for a cost-effective, scalable, and resource-efficient intrusion detection system capable of predicting and addressing diverse cyber-attacks in lightweight drone networks. The X-CID framework demonstrated superior performance in detecting cyber-intrusions across three benchmark datasets. Notably, it achieved a 1.05% improvement in F1-score and 0.25% higher accuracy compared to the best-performing traditional model (decision tree) on the WSN-DS dataset. Furthermore, the prediction error (MSE) was reduced by 33.3%, ensuring a higher level of reliability in intrusion detection. Although X-CID incurs a higher detection latency (e.g., 32.4 s compared to 0.392 s for DT), this trade-off is justified by the significantly higher precision (99.84%) and its ability to process more complex traffic features. However, as noted in Section 4.5, while X-CID effectively detects behavioral anomalies within the network, the current framework does not explicitly mitigate identity spoofing or drone impersonation attacks at the authentication stage. Addressing this limitation through zero-trust access control, device fingerprinting, and blockchain-based identity management presents a promising direction for future research. Also, introducing anthropomorphic cyber-intrusion characteristics into the design to unbox its decision logics will complement its safety. Overall, the MINDS framework advances the field of secure aerial networking and provides a scalable, intelligent baseline for the next generation of autonomous drone systems.

Author Contributions

Simeon Okechukwu Ajakwe: conceptualization, data curation, formal analysis, investigation, methodology, project administration, software, supervision, validation, visualization, writing – original draft, writing – review & editing. **Kazeem Lawrence Olabisi:** conceptualization, data curation, formal analysis, investigation, validation, visualization, writing – original draft, writing – review & editing. **Dong-Seong Kim:** Formal analysis, funding acquisition, investigation, project administration, resources, supervision, validation, writing – review & editing.

Acknowledgements

This research was supported by the Priority Research Centers Program through the NRF funded by the MEST (2018R1A6A1A03024003) (30%) and this work was supported by the IITP (Institute of Information Coummunications Technology Planning Evaluation)-ITRC (Information Technology Research Center) grant funded by the Korea government (Ministry of Science and ICT) (IITP-2025-RS-2024-00438430, 30%). This work was supported by the Institute of Information & Communications Technology Planning & Evaluation (IITP)-Innovative Human Resource Development for Local Intellectualization program grant funded by the Korea government (MSIT) (IITP-2025-RS-2020-II201612, 40%).

Conflicts of Interest

The authors declare that there is no conflicts of interest in this document.

Data Availability Statement

Data sharing is not applicable—no new data is generated, or the article describes entirely theoretical research.

References

1. Y. Li, M. Liu, and D. Jiang, "Application of Unmanned Aerial Vehicles in Logistics: A Literature Review," *Sustainability* 14, no. 21 (2022): 14473.

2. S. Ajakwe, D. S. Kim, and J.-M. Lee, "Radicalization of Airspace Security: Prospects and Botheration of Drone Defense System Technology," *The Journal of Intelligence, Conflict, and Warfare* 6, no. 1 (2023): 23–48.

3. L. Cui, C. Xu, S. Yang, et al., "Joint Optimization of Energy Consumption and Latency in Mobile Edge Computing for Internet of Things," *IEEE Internet of Things Journal* 6, no. 3 (2018): 4791–4803.

4. S. O. Ajakwe and D.-S. Kim, "Facets of Security an Safety Problems and Paradigms for Smart Aerial Mobility and Intelligent Logistics," *IET Intelligent Transport Systems* 18, no. S1 (2024): 2827–2855.

5. A. R. Javed, F. Shahzad, S. ur Rehman, et al., "Future Smart Cities: Requirements, Emerging Technologies, Applications, Challenges, and Future Aspects," *Cities* 129 (2022): 103794.

6. U. Inayat, M. F. Zia, S. Mahmood, H. M. Khalid, and M. Benbouzid, "Learning-Based Methods for Cyber Attacks Detection in IoT Systems: A Survey on Methods, Analysis, and Future Prospects," *Electronics* 11, no. 9 (2022): 1502.

7. X. Dong, Z. Yu, W. Cao, Y. Shi, and Q. Ma, "A Survey on Ensemble Learning," *Frontiers of Computer Science* 14, no. 2 (2020): 241–258.

8. H. Nawaz, H. M. Ali, and A. A. Laghari, "UAV Communication Networks Issues: A Review," *Archives of Computational Methods in Engineering* 28, no. 4 (2021): 68–73.

9. A. A. Alquwayzani and A. A. Albuali, "A Systematic Literature Review of Zero trust architecture for UAV Security Systems in IoBT" (2024), doi: 10.20944/preprints202403.0349.v1.

10. S. O. Ajakwe, V. U. Ihekoronye, D.-S. Kim, and J. M. Lee, "DRONET: Multi-Tasking Framework for Real-Time Industrial Facility Aerial Surveillance and Safety," *Drones* 6, no. 2 (2022).

11. S. O. Ajakwe, D.-S. Kim, and J.-M. Lee, "Drone Transportation System: Systematic Review of Security Dynamics for Smart Mobility," *IEEE Internet of Things Journal* 10, no. 16 (2023): 14 462–14 482.

12. S. Ouiazzane, B. Fatimazahra, and M. Addou, "Towards a Multi-Agent Based Network Intrusion Detection System for a Fleet of Drones," *International Journal of Advanced Computer Science and Applications* 11, no. 10 (2020).

13. O. Ceviz, P. Sadioglu, and S. Sen, "A Survey of Security in Uavs and Fanets: Issues, Threats, Analysis of Attacks, and Solutions," *arXiv preprint arXiv:2306.14281* (2023).

14. M. Tropea, M. G. Spina, A. Lakas, P. Sarigiannidis, and F. De Rango, "Secgpsr: A Secure Gpsr Protocol for Fanet Against Sybil and Gray Hole Attacks," *IEEE Access* 12 (2024): 186909–186925.

15. S. O. Ajakwe, C. A. Okoloegbo, J. M. Lee, and D. S. Kim, "Machine Learning Models for Drone Security: Cognitive Versus Cyber Intelligence

for Safety Operations," in *Machine Learning for Drone-Enabled IoT Networks* (Springer, 2025), 121–139.

16. S. S. Panwar, Y. P. Raiwani, and L. S. Panwar, "An Intrusion Detection Model for Cicids-2017 Dataset Using Machine Learning Algorithms," in *2022 International Conference on Advances in Computing, Communication and Materials (ICACCM)* (IEEE, 2022), 1–10.

17. W. Xu, J. Jang-Jaccard, A. Singh, Y. Wei, and F. Sabrina, "Improving Performance of Autoencoder-Based Network Anomaly Detection on Nsl-Kdd Dataset," *IEEE Access* 9 (2021): 140 136–140 146.

18. J. Whelan, T. Sangarapillai, O. Minawi, A. Almehmadi, and K. El-Khatib, "Novelty-Based Intrusion Detection of Sensor Attacks on Unmanned Aerial Vehicles," in *Proceedings of the 16th ACM Symposium on QoS and Security for Wireless and Mobile Networks* (Association for Computing Machinery, 2020), 23–28.

19. S. O. Ajakwe and D.-S. Kim, "Time Sensitive Anti-Infoswarm Agnostic Intelligence for Safe Uav Communication," in *2024 15th International Conference on Information and Communication Technology Convergence (ICTC)* (IEEE, 2024), 1614–1619.

20. O. Valikhanli, "Uav Networks Dos Attacks Detection Using Artificial Intelligence Based on Weighted Machine Learning," *Results in Control and Optimization* 16 (2024): 100457.

21. A. Puder, M. Zink, L. Seidel, and E. Sax, "Hybrid Anomaly Detection in Time Series by Combining Kalman Filters and Machine Learning Models," *Sensors* 24, no. 9 (2024): 2895.

22. M. Asghari, A. Ameli, M. Ghafouri, and M. N. Uddin, "Application of State Observers and Filters in Protection and Cyber-Security of Power Grids," *Smart Cyber-Physical Power Systems: Fundamental Concepts, Challenges, and Solutions* 1 (2025): 451–503.

23. J. Whelan, A. Almehmadi, and K. El-Khatib, "Artificial Intelligence for Intrusion Detection Systems in Unmanned Aerial Vehicles," *Computers and Electrical Engineering* 99 (2022): 107784.

24. R. A. Ramadan, A.-H. Emara, M. Al-Sarem, and M. Elhamahmy, "Internet of Drones Intrusion Detection Using Deep Learning," *Electronics* 10, no. 21 (2021): 2633.

25. B. Fraser, S. Al-Rubaye, S. Aslam, and A. Tsourdos, "Enhancing the Security of Unmanned Aerial Systems Using Digital-Twin Technology and Intrusion Detection," in *2021 IEEE/AIAA 40th Digital Avionics Systems Conference (DASC)* (IEEE, 2021), 1–10.

26. A. M. Awad, K. M. Ali Alheeti, and A. K. A. Najem, "Model Based Anomaly Detection in Cyber Physical Power Systems," in *AIP Conference Proceedings* 3207, no. 1. (AIP Publishing, 2024).

27. H. Shafei, M. Farhangi, R. P. Aguilera, et al., "A Novel Cyber-Attack Detection and Mitigation for Coupled Power and Information Networks in Microgrids Using Distributed Sliding Mode Unknown Input Observer," *IEEE Transactions on Smart Grid* 16, no. 2 (2025): 1667–1681.

28. M. M. Ahsan, M. S. Ali, and Z. Siddique, "Enhancing and Improving the Performance of Imbalanced Class Data Using Novel Gbo and Ssg: A Comparative Analysis," *Neural Networks* 173 (2024): 106157.

29. S. O. Ajakwe, O. Deji-Oloruntoba, S. O. Olatunbosun, F. X. Duorinaah, and I. A. Bayode, "Multidimensional Perspective to Data Preprocessing for Model Cognition Verity: Data Preparation and Cleansing-Approaches for Model Optimal Feedback Validation," in *Recent Trends and Future Direction for Data Analytics* (IGI Global, 2024), 15–57.

30. H. Vaisocherova, I. Almomani, B. Al-Kasasbeh, and M. AL-Akhras, "WSN-DS: A Dataset for Intrusion Detection Systems in Wireless Sensor Networks," *Journal of Sensors* 2016 (2016): 4731953, https://doi.org/10.1155/2016/4731953.

31. I. Sharafaldin, A. Habibi Lashkari, and A. A. Ghorbani, "A Detailed Analysis of the CICIDS2017 Data Set," in *Information Systems Security and Privacy* (Springer International Publishing, 2019).

32. M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A Detailed Analysis of the KDD CUP 99 data set," in *2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications* (IEEE, 2009), 1–6.