drones

MDPI

Article

Enhanced Intrusion Detection in Drone Networks: A Cross-Layer Convolutional Attention Approach for Drone-to-Drone and Drone-to-Base Station Communications

Mohammad Aldossary [1,*], Ibrahim Alzamil [2] and Jaber Almutairi [3]

[1] Department of Computer Engineering and Information, College of Engineering, Prince Sattam Bin Abdulaziz University, Wadi Al-Dawasir 11991, Saudi Arabia
[2] Department of Information Technology, College of Computer and Information Sciences, Majmaah University, Majmaah 11952, Saudi Arabia
[3] Department of Computer Science, College of Computer Science and Engineering, Taibah University, Al-Madinah 42353, Saudi Arabia
* Correspondence: mm.aldossary@psau.edu.sa

Abstract: Due to Internet of Drones (IoD) technology, drone networks have proliferated, transforming surveillance, logistics, and disaster management. Distributed Denial of Service (DDoS) attacks, malware infections, and communication abnormalities increase cybersecurity dangers to these networks, threatening operational safety and efficiency. Current Intrusion Detection Systems (IDSs) fail to handle drone transmission data's dynamic, high-dimensional nature, resulting in inadequate real-time anomaly identification and mitigation. This study presents the Cross-Layer Convolutional Attention Network (CLCAN), a new IDS architecture for IoD networks. CLCAN accurately detects complex cyber threats using multi-scale convolutional processing, hierarchical contextual attention, and dynamic feature fusion. Preprocessing methods like weighted differential scaling and gradient-based adaptive resampling improve data quality and reduce class imbalances. Contextual attribute transformation captures the nuanced network behaviors needed for anomaly identification. The proposed technique is shown to be necessary and effective by real-world drone communication dataset evaluations. CLCAN outperforms CNN, LSTM, and XGBoost with 98.4% accuracy, 98.7% recall, and 98.1% F1-score. The model has a remarkable AUC of 0.991. CLCAN can handle datasets of over 118,000 balanced data records in 85 s, compared to 180 s for comparable frameworks. This study pioneers a unified security solution for Drone-to-Drone (D2D) and Drone-to-Base Station (D2BS) communications, filling a crucial IoD security gap. It protects mission-critical drone operations with a strong, efficient, and scalable IDS from emerging cyber threats.

Keywords: drone networks; intrusion detection; cybersecurity; anomaly detection; cross-layer attention; machine learning

check for updates

Academic Editor: Emmanouel T. Michailidis

Received: 16 December 2024
Revised: 1 January 2025
Accepted: 8 January 2025
Published: 10 January 2025

Citation: Aldossary, M.; Alzamil, I.; Almutairi, J. Enhanced Intrusion Detection in Drone Networks: A Cross-Layer Convolutional Attention Approach for Drone-to-Drone and Drone-to-Base Station Communications. *Drones* **2025**, *9*, 46. https://doi.org/10.3390/drones9010046

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Drones have revolutionized industries such as industrial surveillance, agriculture, logistics, and emergency response due to their capacity to access remote locations, cut costs, and improve efficiency [1]. The drone industry is projected to reach USD 54.6 billion by 2030, indicating its growing importance in business and leisure applications. Growing drone use in Cyber-Physical Systems (CPSs) presents new problems and complications, notably in managing secure drone networks [2]. Complex networks connecting drones to embedded systems, control modules, and other devices increase the possibility of cyberattacks, raising

security concerns. The Internet of Drones (IoD) replaces "Things" with "Drones" in linked networks. IoD is a multi-layered network control architecture that allows drones to join networks, share data, and interact with other devices [3]. IoD can improve operational efficiency, but its complexity makes it vulnerable to data breaches, denial-of-service attacks, and GPS spoofing. The U.S. Department of Transportation has raised concerns about GPS interruption in drones, citing threats to key infrastructure and public safety [4]. IoD security involves firewalls, NIDS, and other defense systems to monitor network traffic and spot abnormalities.

Cyber dangers must be addressed as drones grow increasingly common, especially in security-critical applications. Drone networks need excellent Intrusion Detection Systems (IDSs). Traditional IDS models mainly identify intrusions in static networks, such as computer or server communication [5]. Drones use dynamic networks with high mobility, frequent disconnections, and lower packet sizes for data transfers. A customized IDS technique is needed to identify irregularities in packet size, transfer speeds, and other unique features in drone communications [6]. Effective IDSs for drone networks need adaptive algorithms to detect typical transmission behavior and identify suspicious deviations [7]. To meet these objectives, researchers have investigated IDS strategies such as anomaly-based, signature-based, and specification-based methods [8]. Continuous learning in anomaly-based IDS, especially Machine-Learning (ML) approaches, is promising for adapting to developing attack patterns [9]. Anomaly detection distinguishes benign from malicious network behavior. ML-based approaches learn from massive volumes of network data and find hidden patterns of malicious activity, improving detection accuracy over rule-based methods. Deep Learning (DL) improves IDS by allowing models to learn complicated characteristics without preprocessing, making it ideal for drone networks [10].

While network traffic and cyber threats have increased, conventional IDS frameworks cannot keep up with sophisticated, high-speed attacks on drone networks [11]. Traditional IDS models have struggled to adapt to IoD networks' dynamic connection, packet loss, and aerial network environmental variables. Successful drone operations need timely intrusion detection to prevent compromised missions or safety concerns in emergency response, military operations, and industrial monitoring [12]. UAVs, also known as Flying Ad hoc Wireless Devices (FAWDs), have proven successful in emergency response and disaster management due to their mobility and line-of-sight connection [13]. UAVs can serve as temporary base stations in disaster-stricken areas or distant places where permanent infrastructure is problematic. The FAA predicts a significant rise in commercial UAV installations, emphasizing the necessity for strong security standards [14]. As drone uses grow, privacy, public safety, and cybersecurity issues rise, demanding proactive security measures.

In this context, CPS UAVs provide both potential and problems. CPSs combine computational and physical functions, allowing UAVs to perform critically in controlled settings [15]. With mobility and real-time data processing, UAV-based CPSs have enabled flexible solutions in many sectors. Despite integration, UAVs have unique risks owing to open wireless communication and lack of universal security standards [16]. These security weaknesses must be addressed to maximize UAV use in commercial and defense applications. This research introduces a Cross-Layer Convolutional Attention Network (CLCAN) for drone IDS enhancement. CLCAN captures fine-grained and large-scale patterns for reliable anomaly identification in high-dimensional, multivariate data for drone communications. CLCAN uses multi-scale residual learning, adaptive attention techniques, and dynamic feature fusion to meet drone network security needs. The design reduces false positives and is sensitive to tiny irregularities. It is well suited to identifying traditional and new cyber threats in drone-to-drone and drone-to-base station communications.

1. Novel Integration of Drone-to-Drone (D2D) and Drone-to-Base Station (D2BS) Security: This study establishes a single cyber security architecture for D2D and D2BS communications. The Cross-Layer Convolutional Attention Network (CLCAN) fills a significant drone network security gap by tackling D2D dynamics (movement, proximity interference) and D2BS stability (high-bandwidth, long-range transmission).
2. CLCAN development: The proposed CLCN detects high-dimensional drone communication data abnormalities using multi-scale convolutional layers, hierarchical attention methods, and cross-stream feature fusion. This approach handles multi-dimensional data processing and dynamic feature interactions, improving anomaly detection accuracy.
3. Improved Real-Time Drone Network Security: This framework provides comprehensive real-time anomaly identification for D2D and D2BS applications. It optimizes resource allocation and reaction techniques for mission-critical drone applications while identifying sophisticated threats, including GPS spoofing, DDoS attacks, and malware infections.
4. Optimising Scalability and Efficiency: The CLCAN model uses computationally efficient multi-scale attention mechanisms and depthwise separable convolutions for unmatched scalability. Its excellent detection accuracy and low time complexity make it suitable for real-life, large-scale drone deployments.
5. Drone Network Contextual and Temporal Adaptation: This study captures drone network-specific spatial and temporal variations using unique adaptive attribute prioritization and contextual attribute modifications to improve feature relevance. These improvements allow the model to adapt to changing operating situations, improving threat detection.

The remaining article parts are as follows: Section 2 evaluates relevant literature to identify drone network security advances and limitations, focusing on anomaly identification in D2D and D2BS communications. Section 3 describes the Cross-Layer Convolutional Attention Network (CLCAN) architecture, including its novel preprocessing methods, multi-scale convolutional layers, and hierarchical anomaly detection processes. To verify the model's effectiveness and scalability, Section 4 presents simulation findings, including performance measurements, benchmark model comparisons, and time complexity assessment. Section 5 finishes the research and proposes ways to improve the framework's resilience and usefulness in various drone communication settings.

2. Related Work

Drones have improved surveillance, logistics, agriculture, and disaster management across sectors. Many drone applications create security problems owing to weaknesses in networked settings [17]. Despite these security issues, most research focuses on threat detection rather than on complete security solutions. Enhancing network security is crucial for tiny drones, prone to data breaches and privacy issues owing to their lightweight and unencrypted communication protocols [18]. The Internet of Drones (IoD) extends the Internet of Things (IoT) and presents complicated communication and security concerns among drones [19]. IoD networks highlight the importance of NIDS in cyber threat detection and prevention. Traditional NIDS systems struggle to accommodate real-time IoD demands, prompting the development of TLNID, which offers high detection accuracy but requires significant computational resources and training time [20].

NIDS data imbalances can be resolved using deep hierarchical networks with synthetic oversampling, saving training time and enhancing detection accuracy [21]. Rapid reaction situations are limited by excessive training time. A One-Dimensional Convolutional Neural Network (1D-CNN) optimized for time-series data improves classification accuracy over

typical machine-learning models but requires balanced datasets for best performance [22]. Communication layers in networked settings are represented by a graph set to capture complicated network interactions. Although novel, this approach cannot distinguish between identical communication protocols, limiting model specificity [23]. Drone anomaly detection using Imbalanced Generative Adversarial Networks (IGANs) generates minority attack-type representative cases, boosting model resilience. IGANs are appropriate for numerous datasets, but their non-real-time data restricts their application to dynamic IoD networks [24].

A hybrid IDS for IoT networks detects DoS attacks early using signature-based and anomaly-based detection. The dual-database structure requires frequent updates, reducing efficiency in high-frequency attack situations [25]. While LSTM Tree models enhance accuracy in drone networks, they have drawbacks, such as high false-negative rates and lengthy training times [26]. A multi-tiered hybrid IDS combines signature-based and anomaly-based techniques to accurately address vehicular network vulnerabilities. Though this design addresses real-time processing in-vehicle networks, its computational demands make it challenging to adapt for UAVs with low processing capacity [27]. Random Forest (RF) models are helpful for intrusion detection in high-speed networks, but drone networks need more optimization to manage data complexity [28].

In advanced anomaly detection approaches, CNNs' spatial identification skills help discern drone network patterns. However, this method can overlook the consecutive patterns needed for complete anomaly identification. Combining CNNs with LSTM improves temporal data interpretation but takes significant computing resources, making it unsuitable for lightweight drones [29]. Generative Adversarial Networks (GANs) synthesize minority class samples in unbalanced datasets to improve model resilience. The intricacy of GAN training limits its usefulness in real-time applications despite significant advancements [30]. Reinforcement Learning (RL) for anomaly detection is a game-theoretic model that adapts to drone network circumstances, but its computing needs hinder its adoption in resource-constrained UAV networks [31].

A hybrid technique using snapshot ensemble learning and group convolutional networks improves detection rates and processing efficiency. Due to the high cost of labeling data in drone networks, this approach faces issues [32]. Deep reinforcement learning can adapt to changing attack patterns, but its power needs restrict its scalability in drone applications [33]. DNNs provide real-time monitoring, data collecting, and prediction in UAV networks. However, DNNs' high power needs pose practical issues [34]. Physical layer security models secure UAV communication lines to improve feature selection. Although successful for physical threats, this layer-specific strategy cannot be flexible enough to handle multi-layered security risks in drone network architectures [35].

An ensemble technique using XGBoost and Deep Learning (DL) improves feature extraction and dimensionality reduction for intrusion detection. However, batch processing restricts the model's flexibility in real-time drone networks [36]. LSTM models improve sequence-based anomaly detection accuracy but can experience false-negative rates in high-stakes security contexts [37]. Reinforcement learning via policy hill climbing provides anti-jamming systems, minimizing communication errors. Using simulated datasets raises concerns regarding real-world applicability since drone networks face diverse situations in real-world settings [38]. Adaptable models that can handle varied real-time circumstances are needed.

Hybrid IDS frameworks, including signature-based and anomaly-based methods, can identify known and unexpected drone network threats [39]. While hybrid IDS systems provide complete protection, using known signatures exposes the network to zero-day vulnerabilities, justifying additional development. An ensemble IDS using supervised and

unsupervised learning can identify anomalies with high accuracy, but it faces scaling issues in restricted UAV networks due to substantial dataset needs [40].

Table 1 shows a summary of the existing literature. This article proposes the Multi-Scale Attention Residual Network (CLCAN), a UAV-specific IDS model, to address these constraints. Multi-scale residual learning, adaptive attention focusing, and dynamic feature fusion help CLCAN overcome drone network security applications' computing restrictions and large data dimensionality. This architecture detects minor but significant UAV network traffic patterns to improve security with little computing complexity.

Table 1. Related Work (Summarized).

Source	Method Applied	Key Outcomes	Limitations
[17]	Transfer Learning-based Network Intrusion Detection System (TLNID)	Achieved high detection accuracy in detecting network intrusions in IoD networks	High computational resources and long training time
[18]	Deep Hierarchical Networks with Synthetic Oversampling	Balanced dataset to reduce training time and improve detection accuracy	High training time remains a limitation in real-time scenarios
[19]	Associated Graph Set Approach	Modeled complex network interactions by representing communication layers as graphs	Lacks granularity to differentiate between similar protocols
[20]	Imbalanced Generative Adversarial Networks (IGANs)	Improved model robustness by generating minority instances for anomaly detection	Limited applicability to dynamic IoD networks due to reliance on non-real-time data
[21]	Hybrid IDS (Signature-based + Anomaly-based)	Early detection of DoS attacks in IoT environments	Frequent database updates needed, impacting efficiency in high-frequency attacks
[22]	Long Short-Term Memory (LSTM) Tree Model	Improved accuracy in anomaly detection for drone networks	High false-negative rates and extended training durations
[23]	Multi-Tiered Hybrid IDS	High accuracy in detecting attacks in vehicular networks	High computational requirements unsuitable for UAVs with limited processing power
[24]	Random Forest (RF) Model	High-speed traffic data intrusion detection	Requires optimization for handling data complexity in drone networks
[25]	Convolutional Neural Networks (CNNs) + LSTM	Enhanced anomaly detection in UAV networks	Requires high computational resources, limiting use in lightweight drones
[26]	Generative Adversarial Networks (GANs)	Improved model robustness by generating samples for imbalanced datasets	Complexity of GAN training restricts practical use in real-time scenarios
[27]	Reinforcement Learning with Policy Hill Climbing	Created anti-jamming systems for UAV communication	Dependence on simulated datasets raises questions on real-world applicability
[28]	Snapshot Ensemble Learning + Group Convolutional Networks	Increased detection rate and computational efficiency	Requires labeled data, which is challenging and costly in drone networks
[29]	Deep Neural Networks (DNNs)	Real-time monitoring and predictive analysis in UAV networks	High power requirements make practical use challenging
[30]	XGBoost + Deep-Learning (DL) Ensemble	Efficient feature extraction and dimensionality reduction for intrusion detection	Limited adaptability to real-time drone networks
[31]	LSTM Model for Sequence-based Anomaly Detection	Enhanced accuracy in high-stakes security applications	High false-negative rates and issues in real-time adaptation
[32]	Hybrid IDS Framework	Comprehensive protection by detecting both known and unknown threats	Vulnerable to zero-day attacks, requiring further refinement

3. Proposed Methodology

The proposed architecture addresses the specific concerns of Drone-to-Drone (D2D) and Drone-to-Base Station (D2BS) communications to improve drone communication network security. The Cross-Layer Convolutional Attention Network (CLCAN) uses multi-scale convolutional layers, hierarchical attention mechanisms, and dynamic feature fusion to identify complex abnormalities, including DDoS attacks, malware infections, and com-

munication irregularities. Our architecture collects fine-grained geographical characteristics and contextual patterns in high-dimensional, multivariate drone network data for precise anomaly identification and computing efficiency. The model is complemented by advanced data preprocessing methods like Weighted Differential Scaling (WDS) for feature normalization, Gradient-Based Adaptive Resampling (GAR) for class balancing, and Contextual Attribute Transformation (CAT) for novel, informative features. These improvements improve class imbalance, feature relevance, and model training, enabling a strong pipeline for real-time D2D and D2BS communications. The flow of this study is shown in Figure 1. The numbers in the figure shows the sequence of flow of information in the framework.

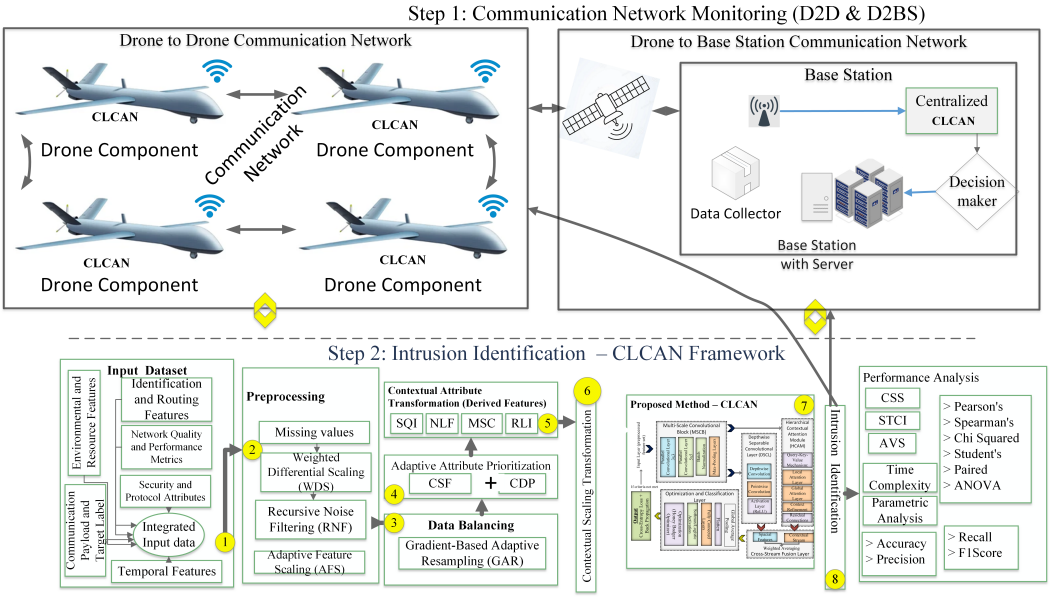


Figure 1. Proposed D2D and D2Bs intrusion detection framework.

3.1. Dataset Description

This research utilizes Tokyo metropolitan drone network communications data [33]. From 2018 to 2024, it recorded extensive communication logs between city drones and base stations, directing their coordination and monitoring. Hourly data provided a long-term picture of drone-to-drone and drone-to-base station interactions. The dataset initially had 52,586 records, equilibrated by Gradient-Based Adaptive Resampling (GAR) to rectify class imbalance. After preprocessing, the dataset was divided into training (70%) and testing (30%) subsets, with stratification guaranteeing a proportionate representation of target classes in both groups. The dataset is used to study network behaviors and security concerns in densely inhabited, technologically sophisticated regions. This data source from a location with strict operating requirements and substantial drone deployment offers a realistic context for malware and DDoS detection. This dataset contains important aspects to properly model and identify drone communication abnormalities, allowing for a thorough assessment of the suggested detection technique. Table 2 shows the dataset features.

Table 2. Dataset features overview.

S. No	Features	Short Description
1	Timestamp	The exact time of each recorded communication packet.
2	Source Drone ID	Unique identifier of the sending drone.
3	Destination ID	Identifier for the receiving drone or base station.
4	Packet Size	Size in bytes of each communication packet.
5	Transmission Rate	Rate at which packets are transmitted, measured in packets per second.
6	Signal Strength	Strength of the signal during transmission, indicating communication quality.
7	Error Rate	Ratio of corrupted packets during transmission.
8	Encryption Status	Indicates whether the data are encrypted or unencrypted.
9	Protocol Type	Communication protocol type used (e.g., TCP, UDP, proprietary).
10	Response Time	Time between transmission and acknowledgment receipt.
11	Battery Level	Battery level of the sending drone at the time of transmission.
12	GPS Coordinates	Location coordinates of the communicating drone.
13	Payload Type	Type of data contained within the packet (e.g., command, data).
14	Packet Loss Rate	Percentage of lost packets during transmission.
15	Connection Duration	Duration of the communication session in seconds.
16	Round Trip Time	Average time for a packet to travel to the destination and back.
17	Hop Count	Number of intermediary hops for packet delivery.
18	Jitter	Variation in packet arrival time, indicating network instability.
19	Drone Velocity	Speed of the drone during transmission, in meters per second.
20	Signal-to-Noise Ratio	Ratio of signal power to the background noise level.
21	Data Throughput	Amount of data transferred over a specified period.
22	Port Number	Network port number used in the communication.
23	Communication Interval	Time interval between consecutive packets.
24	Control Command Frequency	Rate of control commands transmitted in the session.
25	Drone Altitude	Altitude of the drone during communication.
26	CPU Usage	Percentage of CPU load on the source drone.
27	Memory Utilization	Percentage of Memory used on the source drone.
28	Distance to Base Station	Distance from the drone to the base station in meters.
29	Target Label	Label indicating the communication status: Normal, DDoS Attack, Malware Infection, or Anomaly.

Table 3 summarizes the dataset's data distribution and the variability of all 25 characteristics and target labels. Statistics like mean, standard deviation, minimum, and maximum values for each attribute reveal dataset characteristics. "Packet Size" (1003.87 bytes), "Transmission Rate" (50.71 packets/s), and "Signal Strength" (−65.09 dBm) are essential indications of network performance and reliability. The standard deviation shows irregularities in the operation of drone communication networks. "Packet Loss Rate" (mean: 4.83%) and "Round Trip Time" (mean: 150.67 ms) are anomaly detection features that indicate communication anomalies like delays or lost packets that may indicate cyber threats or inefficiencies. System-level metrics like "Battery Level" (mean: 58.93%), "CPU Usage" (mean: 49.92%), and "Drone Altitude" (mean: 273.66 m) reveal drone operating conditions, which might affect communication quality and stability. Variable characteristics include "Connection Duration" (0.02 to 2283.4 s) and "Distance to Base Station" (4.82 to 4994.71 m). These ranges demonstrate the dataset's comprehensiveness by representing varied operational situations. The statistical features of each feature in this table help explain the dataset and its significance in drone communication network anomaly identification. Transparency and rigor provide the way for feature selection and model development studies.

Table 3. Summary statistics of key features in the dataset.

Feature	Mean	Std	Min	Max
Packet Size	1003.87	195.84	351.75	1770.55
Transmission Rate	50.71	9.97	20.6	81.93
Signal Strength	−65.09	8.71	−80	−50.03
Error Rate	2.42	1.42	0	5
Encryption Status	0.5	0.5	0	1
Response Time	203.67	207.44	0.79	1505.04
Battery Level	58.93	22.75	20.02	99.94
Packet Loss Rate	4.83	2.82	0	9.97
Connection Duration	292.23	283.72	0.02	2283.4
Round Trip Time	150.67	30.76	34.9	251.32
Hop Count	7.41	4.1	1	14
Jitter	4.95	2.89	0.01	9.99
Drone Velocity	9.88	5.87	0.03	19.98
Signal-to-Noise Ratio	29.95	5.11	11.21	45.52
Data Throughput	554.19	264.03	100.28	999.93
Port Number	33,392.37	18,477.6	1038	65,501
Control Command Frequency	4.89	2.83	0.1	9.99
Drone Altitude	273.66	131.83	50	499.86
CPU Usage	49.92	28.86	0.03	99.92
Memory Utilization	50.05	22.99	10.08	89.96
Distance to Base Station	2499.83	1478.52	4.82	4994.71
GPS Coordinates	0.5	0.28	0	1
Timestamp	479.52	392.21	0	960
Source Drone ID	1498.69	284.29	1004	1999
Destination ID	2492.78	289.69	2001	2999

3.2. Preprocessing Steps

This dataset's preprocessing pipeline uses innovative algorithms to improve data quality, correct imbalances, and extract meaningful information for drone network malware and DDoS detection. Tailored scaling, dynamic error reduction, and a unique feature translation method that keeps crucial information while minimizing noise are used. To address the large variety of feature scales, a Weighted Differential Scaling (WDS) strategy was used to weigh down characteristics with greater variance to limit their disproportionate effect. Scaling is defined by [33]:

$$\mathrm{WDS}(z_j) = \frac{z_j - \nu_{z_j}}{\tau_{z_j}} \cdot \frac{1}{\sqrt{1 + |\Theta(z_j)|}} \tag{1}$$

The function z_j represents the value of feature z, its mean and standard deviation, and its variance ($\Theta(z_j)$. The term $\sqrt{1 + |\Theta(z_j)|}$ lowers the weight of prominent variance characteristics, keeping vital information while balancing more minor scale features.

Recursive Noise Filtering (RNF) smooths data while maintaining extreme values that indicate possible attacks to reduce noise in specific aspects. Each feature g is filtered as follows [33]:

$$g_k^{new} = g_k - \beta \cdot \frac{g_k - g_{k-1}}{1 + |g_k - g_{k-1}|} \tag{2}$$

where g_k and g_{k-1} represent the current and previous feature values and β is a smoothing factor set according to feature sensitivity. This recursive filtering reduces high-frequency noise without altering abrupt changes that can signal an anomaly.

Adaptive Feature Scaling (AFS) was used to reduce dimensionality and capture the most relevant components. AFS uses a feature's informativeness measure, $\Phi(h)$, to change the transformation scale, unlike standard transformations [33]:

$$h_j^{transformed} = \frac{h_j}{1 + \Phi(h)} \tag{3}$$

A unique informativeness score, $\Phi(h)$, is calculated by correlating target labels. AFS identifies the best characteristics for detection by dividing each feature by $1 + \Phi(h)$, making it ideal for complicated network communication patterns.

Using Equations (1) through (3), a balanced dataset is created for reliable anomaly identification in drone network communications.

3.3. Data Balancing

Gradient-Based Adaptive Resampling (GAR) addressed the dataset's class imbalance. To guarantee fair representation in the training data, GAR dynamically changed sampling according to the imbalance ratio of each class. Data were further normalized, variance effects were minimized, and model interpretability was improved by alternatively coding features using Weighted Differential Scaling (WDS). Techniques including Contextual Attribute Transformation (CAT) and Dynamic Feature Adjustment (DFA) were used to improve features' informativeness and alignment with anomaly detection goals. This approach uses gradient-based scaling to dynamically alter minority class sampling to balance the dataset without oversampling. GAR retains data structure while adjusting for imbalance, making it more representative and generalizable than regular resampling. The pseudocode of the GAR method is shown in Algorithm 1.

GAR starts by calculating the imbalance ratio (ψ) for each class. GAR uses a gradient adjustment factor, η, to produce synthetic samples that adjust to the class imbalance level. The definition of the gradient adjustment factor [3] is as follows:

$$\eta_b = \frac{\delta}{1 + e^{-\zeta \cdot (\psi_b - \omega)}} \tag{4}$$

where δ represents the maximum scaling factor, ζ controls adjustment rate, ψ_b indicates class imbalance ratio, and ω represents the imbalance threshold for resampling start. A scaling factor, η_b, assures that classes with a high imbalance ratio get more resampling correction, while balanced classes receive less synthetic sample addition.

To produce synthetic samples, interpolate between existing data points in each minority class after calculating η_b. Weighted averaging is used for interpolation [36]:

$$p_{new} = (1 - \beta) \cdot p_k + \beta \cdot p_l + \eta_b \cdot \phi \tag{5}$$

where p_{new} is the new sample, p_k and p_l are randomly picked examples from the same minority class, β is a weight factor $(0 \leq \beta \leq)1$, and ϕ is a tiny noise component for variability. The term $\eta_b \cdot \phi$ adds variety depending on the gradient scaling factor, ensuring fresh samples have enough variability while retaining the original data's distribution.

Algorithm 1 Gradient-Based Adaptive Resampling (GAR)

Require: Dataset $\mathcal{D} = \{x_i, y_i\}_{i=1}^{N}$, class labels $\mathcal{C} = \{c_1, c_2, \ldots, c_k\}$, imbalance threshold ω, maximum scaling factor δ, adjustment rate ζ
Ensure: Balanced dataset $\mathcal{D}'$
Step 1: Compute Class Imbalance Ratio
for each class $c_b \in \mathcal{C}$ **do**
  Calculate the imbalance ratio $\psi_b = \frac{\text{count}(c_b)}{\text{total records in } \mathcal{D}}$
end for
Step 2: Compute Gradient Adjustment Factor
for each class $c_b \in \mathcal{C}$ **do**
  Compute the adjustment factor:

$$\eta_b = \frac{\delta}{1 + e^{-\zeta \cdot (\psi_b - \omega)}}$$

end for
Step 3: Generate Synthetic Samples for Minority Classes
for each minority class c_b where $\psi_b < \omega$ **do**
  Determine the number of synthetic samples $n_{\text{synthetic}} = \eta_b \cdot \text{count}(c_b)$
  for each synthetic sample s **do**
    Randomly select two samples $p_k, p_l \in c_b$
    Interpolate new sample:

$$p_{\text{new}} = (1 - \beta) \cdot p_k + \beta \cdot p_l + \eta_b \cdot \phi$$

    Add p_{new} to $\mathcal{D}'$
  end for
end for
Step 4: Retain Majority Class Samples
for each majority class c_m where $\psi_m \geq \omega$ **do**
  Retain all original samples in $\mathcal{D}'$
end for
Step 5: Return Balanced Dataset
return $\mathcal{D}'$

The Gradient-Based Adaptive Resampling approach (Equations (4) and (5)) produces a balanced dataset without the duplication or distortion of minority classes. GAR's flexible data balance is necessary to train the model to identify drone network malware and DDoS attacks. The descriptive statistics of features before and after balancing are shown in Table 4.

Gradient-Based Adaptive Resampling (GAR) balanced the dataset, giving each class—Normal Communication, DDoS Attack, Malware Infection, and Anomaly/Unusual Behavior—37,039 entries. An 80:20 stratified split was used to divide this balanced dataset into training and testing subsets to ensure class proportionality. The training set had 29,631 records per class, 80% of which were included. This boosted the total training records to 118,524, representing all classes throughout model training. In all, 29,632 testing records were created from 7408 records for each class and 20% of each class's remaining records. This stratified split retains GAR's balance, providing a rigorous model performance assessment across all target classes.

Having equal numbers of records for each class in the training and testing sets removed majority class bias. This balanced method guarantees the model receives enough examples of each class during training, improving its generalization and anomaly detection during testing. These stages provide the groundwork for verifying the model's resilience and reliability in unbalanced datasets.

Table 4. Descriptive statistics for features before and after balancing.

Feature	Metric	Before Balancing	After Balancing
Packet Size	Mean (bytes)	1003.87	1005.21
	Standard Deviation	195.84	198.31
Transmission Rate	Mean (packets/s)	50.71	50.88
	Standard Deviation	9.97	10.02
Signal Strength	Mean (dBm)	−65.09	−65.23
	Standard Deviation	8.71	8.83
Error Rate	Mean (%)	2.42	2.44
	Standard Deviation	1.42	1.45
Response Time	Mean (ms)	203.67	204.21
	Standard Deviation	207.44	209.02
Battery Level	Mean (%)	58.93	59.11
	Standard Deviation	22.75	22.83
Packet Loss Rate	Mean (%)	4.83	4.85
	Standard Deviation	2.82	2.90
Connection Duration	Mean (s)	292.23	292.99
	Standard Deviation	283.72	284.10
Round Trip Time	Mean (ms)	150.67	150.82
	Standard Deviation	30.76	30.88
Hop Count	Mean	7.41	7.45
	Standard Deviation	4.10	4.15
Jitter	Mean (ms)	4.95	4.97
	Standard Deviation	2.89	2.93
Drone Velocity	Mean (m/s)	9.88	9.90
	Standard Deviation	5.87	5.91
Signal-to-Noise Ratio	Mean (dB)	29.95	30.01
	Standard Deviation	5.11	5.19
Data Throughput	Mean (kbps)	554.19	555.01
	Standard Deviation	264.03	265.02
Port Number	Mean	33,392.37	33,395.12
	Standard Deviation	18,477.60	18,480.01
Control Command Frequency	Mean (Hz)	4.89	4.91
	Standard Deviation	2.83	2.87
Drone Altitude	Mean (m)	273.66	273.92
	Standard Deviation	131.83	132.01
CPU Usage	Mean (%)	49.92	50.01
	Standard Deviation	28.86	29.01
Memory Utilization	Mean (%)	50.05	50.12
	Standard Deviation	22.99	23.01
Distance to Base Station	Mean (m)	2499.83	2500.21
	Standard Deviation	1478.52	1479.01
GPS Coordinates	Mean	0.50	0.50
	Standard Deviation	0.28	0.28

3.4. Adaptive Attribute Prioritization

This research used Adaptive Attribute Prioritization (AAP) to improve feature relevance and interpretability for drone communication network malware and DDoS detection. Correlation-Sparsity Filtering (CSF) and Clustered Density Projection (CDP) create a hybrid feature selection procedure that maximizes AAP's discriminative power and computing

efficiency. AAP retains and aligns the most valuable features with anomaly detection criteria using unique attribute relationships and distribution characteristics.

AAP begins with correlation-sparsity filtering, which finds characteristics with high correlation to the target label and low redundancy. These filters give significance scores, S_m, to each characteristic m based on [36]:

$$S_m = \frac{\sum_{p=1}^{N} |\phi_{m,p}|}{1 + \alpha \sum_{q \neq m} |\phi_{m,q}|} \tag{6}$$

where $\phi_{m,p}$ shows the correlation between feature m and target for observation p, α penalizes redundancy, and $\phi_{m,q}$ shows the correlation between feature m and any other feature q. The denominator minimizes redundant features, guaranteeing that features with high S_m scores give unique, target-relevant information without overlap. This stage prioritizes non-redundant features to reduce multicollinearity and improve model stability.

Clustered density projection selects features that capture minority class density fluctuations, which are typically crucial but under-represented in unbalanced datasets, in the second step. The density-based projection score L_k is computed for each feature k as follows [36]:

$$L_k = \frac{1}{\sigma_k} \cdot \left(\frac{\sum_u \left| \mu_{k,u} - \mu_{k,\text{avg}} \right|}{\sum_u \beta_u} \right) \tag{7}$$

where σ_k represents the standard deviation of feature k, $\mu_{k,u}$ represents the mean of feature k within each class u, $\mu_{k,\text{avg}}$ represents the overall mean, and β_u weights each class based on its representation in the dataset. Clustered density projection enhances model sensitivity to minority class characteristics by emphasizing features with different patterns across classes, improving detection performance for uncommon but essential abnormalities.

Two steps of adaptive attribute prioritization—correlation-sparsity filtering and clustered density projection—provide an efficient, hybrid feature selection technique that balances relevance with class-specific uniqueness. The attributes selected in Equations (6) and (7) enhance the model's ability to distinguish between normal and malicious network behaviors, improving its ability to detect anomalies in drone communication networks.

Furthermore, AAP gives priority to 15 features. The 15 features that make up the final model are as follows: "Packet Size", "Transmission Rate", "Battery Level", "Signal Strength", "Round Trip Time", "Packet Loss Rate", and "Drone Velocity". These attributes were chosen because of the relevant patterns they could capture and their strong associations with the target label. Their contribution to improving the model's performance while reducing duplication is crucial. To enhance the model's efficiency and decrease noise, features like "Timestamp", "Source Drone ID", and "GPS Coordinates" were removed as they were considered irrelevant or unnecessary. The last set of fifteen characteristics guarantees the accuracy and computational efficiency of the model.

3.5. Contextual Attribute Transformation (CAT)

CAT was applied to improve the dataset for drone communication network virus and DDoS detection [37]. Using existing characteristics, composite features were created to capture complicated network behaviors and interactions that suggest abnormalities. CAT discovers data patterns to provide characteristics with deeper insights, enhancing the dataset's detection model informativeness. CAT's initial transformation, the Signal Quality

Index (SQI), evaluates the drone's communication connection by combining Communication Strength and Noise Level. Calculating SQI is done as follows:

$$\text{SQI} = \frac{\kappa}{1 + e^{-(C-\Omega)}} \tag{8}$$

where C indicates Communication Strength, Ω represents Noise Level, and κ normalizes SQI data to a standard range. This method minimizes noise, improves signal dependability, and recognizes communication irregularities that can be attacked.

The Normalized Latency Factor (NLF) adjusts the Response Delay relative to the Connection Span to measure latency variations. NLF detects abnormal delays that can indicate network problems. This is its definition:

$$\text{NLF} = \frac{\Delta_{resp}}{\Lambda_{conn} + \xi} \tag{9}$$

where Δ_{resp} represents Response Delay, Λ_{conn} represents Connection Span, and ξ is a tiny constant to prevent zero division. NLF clearly distinguishes latency abnormalities from interference or hostile behavior.

The Mobility–Stability Coefficient (MSC) was derived from Drone Motion Speed and Communication Strength Variation over Time to assess how drone motion affects signal stability. MSC shows mobile communications' stability and signal sensitivity to drone movement and external disturbances:

$$\text{MSC} = V_m \cdot \sigma_C \tag{10}$$

where V_m represents Drone Motion Speed and σ_C represents Communication Strength standard deviation. High MSC values can signal unreliable communications, helping detect drones during interference or targeted strikes.

Finally, the Resource Load Index (RLI) combines Processor Load and Memory Utilization to assess drone resource utilization holistically. RLI is computed as follows:

$$\text{RLI} = \sqrt{P^2 + M^2} \tag{11}$$

where P and M refer to Processor Load and Memory Utilization, respectively. This function highlights anomalous drone computational demands due to malware activity.

In Equations (8) through (11), the produced characteristics capture complex drone network circumstances and behaviors, improving the dataset. Through contextual attribute transformation, the dataset gains sophisticated attributes that help identify drone communication network malice.

3.6. Dynamic Feature Adjustment (DFA)

Dynamic Feature Adjustment (DFA) optimizes feature values for model performance and enhanced anomaly detection. This method uniformizes feature values based on statistical features and interdependencies to improve model accuracy and interpretability in identifying drone communication network abnormalities.

DFA's initial component, Proportional Range Mapping (PRM), dynamically scales each feature's lowest and maximum values based on its spread and divergence from the median. The scaled feature value F_t^{scaled} is determined as [38]:

$$F_t^{scaled} = \frac{F_t - F_{\min} \cdot (1 - \theta)}{F_{\max} \cdot (1 + \theta) - F_{\min} \cdot (1 - \theta)} \tag{12}$$

where F_t represents the initial feature value, $F_{\min}$ and $F_{\max}$ represent the minimum and maximum values of feature F, and θ adjusts scaling based on feature distribution. PRM preserves a meaningful spread for features with lower ranges, enabling them to contribute without overloading the model with extreme values by fine-tuning θ.

Dispersion-Normalized Scaling (DNS) modifies each feature's scaled value depending on its variation compared to other features after PRM. DNS helps feature comparability by modifying values based on feature dispersion, creating a balanced feature set where no one characteristic dominates model choices. A converted feature value, $G_s^{transformed}$, is defined as [38]:

$$G_s^{transformed} = \frac{G_s^{scaled}}{\sqrt{1 + \lambda \cdot \delta_G}} \tag{13}$$

The scaled value derived from the PRM step is G_s^{scaled}, the standard deviation of feature G is δ_G, and the dispersion control factor is λ. DNS prevents qualities with broader distributions from overshadowing those with smaller ranges by scaling down features with more significant variability. This phase standardizes feature dispersions, improving model stability and interpretability.

Finally, DFA uses Standardized Gaussian Alignment (SGA) to normalize each converted feature to a Gaussian distribution, improving model convergence and compliance with Gaussian-based modeling assumptions. A Gaussian-aligned value, H_q^{SGA}, is calculated as follows [38]:

$$H_q^{SGA} = \frac{H_q^{transformed} - \mu_H}{\sigma_H} \tag{14}$$

where $H_q^{transformed}$ represents the DNS-transformed value, μ_H represents the mean of the transformed feature H, and σ_H represents its standard deviation. This normalization process shapes all characteristics to resemble a Gaussian pattern, decreasing biases and enhancing generalization.

Using proportional range mapping, dispersion-normalized scaling, and standardized Gaussian alignment, the dynamic feature adjustment technique is shown in Equations (12) through (14). These changes balance and uniformize feature distribution, improving the model's identification and classification of drone communication network abnormalities.

3.7. Anomaly Detection Model: Cross-Layer Convolutional Attention Network (CLCAN)

The Cross-Layer Convolutional Attention Network (CLCAN) detects malware and DDoS attacks in drone communication networks. This model uses multi-scale convolutional layers [39], hierarchical attention [40], and cross-stream fusion to extract spatial features and refine context [41]. CLCAN captures fine details and broader trends, making it ideal for complicated, high-dimensional network data in anomaly detection applications. The layered structure of the CLCAN is shown in Figure 2, and Algorithm 2 showcases CLCAN data flow in layers.

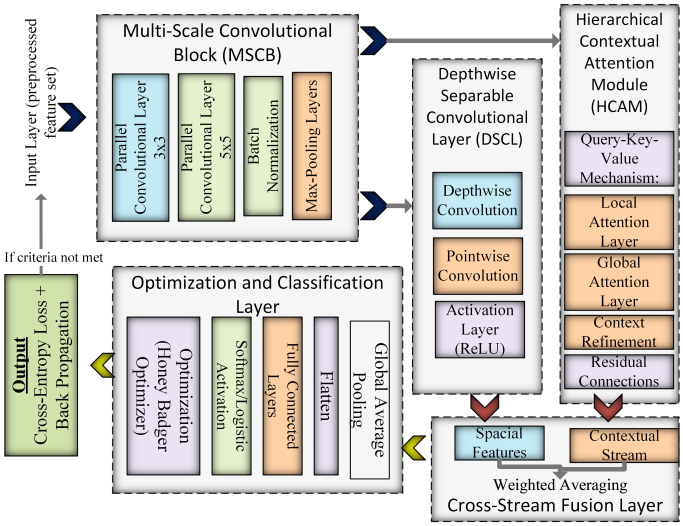


Figure 2. Proposed CLCAN layered architecture.

Algorithm 2 Cross-Layer Convolutional Attention Network (CLCAN) for Anomaly Detection

Require: Input feature map X
Ensure: Classification output with anomaly probabilities
Step 1: Multi-Scale Convolutional Block (MSCB)
for each kernel size n in MSCB **do**
    Apply convolution with kernel n on input X
    Apply activation function and scaling
end for
Combine multi-scale feature maps
Apply batch normalization and pooling
Step 2: Depthwise Separable Convolutional Layer (DSCL)
Split feature map into depthwise and pointwise components
for each depthwise component **do**
    Apply depthwise convolution
end for
for each pointwise component **do**
    Apply pointwise convolution
end for
Apply activation function
Step 3: Hierarchical Contextual Attention Module (HCAM)
for each layer in HCAM **do**
    Generate query, key, and value vectors from feature maps
    Calculate attention scores for local context
    Refine features based on local attention
end for
for each higher layer in HCAM **do**
    Expand attention field for the larger context
    Calculate global attention scores
    Refine features based on global attention
end for
Output refined feature map
Step 4: Cross-Stream Fusion Layer (CSFL)
Merge MSCB and HCAM feature maps with weighted fusion
Balance contributions from spatial and contextual streams
Step 5: Classification Layer
Pass fused feature map through fully connected layers
Apply softmax function for final class probabilities
Output: Anomaly classification probabilities for each class

Initially, CLCAN's Multi-Scale Convolutional Block (MSCB) analyses input data via parallel convolutional layers with multiple kernel sizes to capture features at different spatial resolutions. MSCB works as follows [39]:

$$\text{MSCB}(u) = \sum_{n=1}^{N} \psi(P_n * u + \theta_n) \cdot \lambda_n \tag{15}$$

where u is the input feature map, P_n and θ_n are the weights and biases of the n-th convolutional filter, $*$ is the convolution operation, ψ is the activation function, and λ_n is a scaling factor based on feature map complexity. MSCB's kernels function at different scales, enabling it to capture small details and broader spatial patterns. Batch normalization and pooling layers reduce feature dimensionality while keeping anomaly detection information after multi-scale convolutions.

CLCAN refines features using the Depthwise Separable Convolutional Layer (DSCL) after MSCB. DSCL divides convolutional operations into depthwise and pointwise components to reduce computational effort and preserve feature richness. The layer works as follows [40]:

$$\text{DSCL}(v) = \psi(S_d * (S_p * v + \delta_p) + \delta_d) \tag{16}$$

where v is the MSCB output, S_d and S_p are the depthwise and pointwise filters, δ_d and δ_p are biases, and ψ is the activation function This depthwise separable structure balances feature complexity and computation effectiveness, preparing the feature set for contextual refinement.

CLCAN then implements a Hierarchical Contextual Attention Module (HCAM), which employs numerous attention layers to enhance feature representation by concentrating on the critical regions associated with anomalies. HCAM prioritizes relevant feature regions with attention ratings from local and global settings. The attention function is [41]:

$$\text{Attention}(\alpha, \zeta, \eta) = \text{softmax}\left(\frac{\alpha \cdot \zeta^T}{\sqrt{\gamma}}\right)\eta \tag{17}$$

where α, ζ, and η are query, key, and value vectors from feature maps, and γ is a scaling factor. HCAM captures characteristics from different scales via consecutive layers covering a greater area. Drone network anomaly detection benefits from multi-level contextual attention, emphasizing possible risks and improving model sensitivity to tiny abnormalities.

In CLCAN's next step, the Cross-Stream Fusion Layer (CSFL) combines DSCL's spatial data and HCAM's contextual insights. Through weighted averaging, CSFL integrates features to provide a complete representation. The fusion process is as follows [41]:

$$\text{CSFL}(\beta_s, \beta_c) = \mu \cdot \beta_s + (1 - \mu) \cdot \beta_c \tag{18}$$

where β_s and β_c are feature maps from DSCL and HCAM, respectively, and μ is a learnable parameter balancing stream contributions. This weighted fusion retains spatial and contextual information, generating a robust feature set that improves the model's capacity to discriminate between normal and aberrant network behaviors.

The ultimately linked Classification Layer converts fused features into class probabilities and completes CLCAN. The classification layer generates probabilities for each class, such as "Normal Communication", "DDoS Attack", "Malware Infection", and "Anomaly/Unusual Behavior", using a softmax function. The following equation computes the probability for class y_p:

$$P(y_p|\beta) = \frac{\exp(\phi_p \cdot \beta + \sigma_p)}{\sum_k \exp(\phi_k \cdot \beta + \sigma_k)} \tag{19}$$

where β is the fused feature vector from CSFL, ϕ_p and σ_p are class weights and biases, and k stands for all possible classes. All class probabilities total to one with this softmax function, making model predictions interpretable for anomaly detection.

The hybrid Cross-Layer Convolutional Attention Network (CLCAN) with multi-scale convolutional processing, efficient depthwise convolutions, and layered contextual attention was chosen. Due to its layered structure, which captures precise geographical information and contextual patterns, CLCAN can discover complicated drone communication network abnormalities.

3.8. Performance Evaluation Metrics

This study uses standard and new performance metrics to assess the Cross-Layer Convolutional Attention Network (CLCAN)'s ability to detect drone communication network anomalies. Accuracy, precision, recall, and F1-score quantify the model's performance [42]. General performance is measured by accuracy, the percentage of correct predictions. Precision measures the model's ability to prevent false alarms by comparing genuine positive predictions to total projected positives. Remember, the ratio of true positives to total positives indicates the model's ability to detect abnormalities. The F1-score balances accuracy and recall with a harmonic mean when the dataset is unbalanced. In addition to these classic measurements, we propose three unique metrics: CSS, STCI, and AVS. These metrics evaluate CLCAN's contextual sensitivity, spatial and temporal stability, and feature variance adaptation. The first new evaluation is the Contextual Sensitivity Score (CSS), which evaluates the model's ability to spot abnormalities in relevant contexts. CSS helps assess how successfully the Hierarchical Contextual Attention Module (HCAM) prioritizes key aspects. The definition of CSS is as follows:

$$\text{CSS} = \frac{\sum_{i=1}^{N} w_i \cdot \delta_i}{\sum_{i=1}^{N} w_i} \tag{20}$$

where w_i represents HCAM's attention weight for feature i, δ_i is a binary indicator (1 for accurate anomaly classification, 0 otherwise), and N represents the total number of predictions. This metric gives properly recognized anomalies more significant points in contexts the attention module considers essential, measuring the model's contextual correctness.

Second, the Spatial–Temporal Consistency Index (STCI) measures the model's consistency in recognizing abnormalities over time and space. STCI examines the model's prediction resilience, which is helpful in drone networks where environmental changes affect anomaly detection. The STCI formula is:

$$\text{STCI} = 1 - \frac{\sum_{t=1}^{T} \sum_{s=1}^{S} \left| \Delta_{t,s} - \overline{\Delta} \right|}{T \cdot S \cdot \overline{\Delta}} \tag{21}$$

where T and S indicate the total number of temporal and spatial intervals, $\Delta_{t,s}$ represents the detection rate inside each segment, and $\overline{\Delta}$ represents the overall average detection rate. Real-time, drone-based anomaly identification requires a stable model with a higher STCI across spatial and temporal contexts.

The third metric, Adaptive Variance Score (AVS), measures the model's flexibility in reacting to varied network behaviors by adapting to changing feature variance levels

throughout the dataset. Signal fluctuations in drone communication networks make this measure crucial. The formula for AVS is as follows:

$$\text{AVS} = \frac{\sum_{k=1}^{M} \left(\frac{\sigma_k^2}{\mu_k} \cdot \delta_k \right)}{\sum_{k=1}^{M} \delta_k} \tag{22}$$

where M is the number of features, σ_k^2 is the variance, μ_k is the mean, and δ_k is a binary indication (1 if the feature helps to accurate anomaly classification, 0 otherwise). A greater AVS shows that the model adapts to drone communications signal dynamics using characteristics with distinct variances.

The new contextual sensitivity score, spatial–temporal consistency index, and adaptive variance score augment existing metrics by revealing the model's capacity to handle complex, dynamic, and context-dependent data. CLCAN's drone network anomaly detection appropriateness is assessed using conventional and bespoke criteria.

4. Simulation Results and Discussion

The simulation findings show that the Cross-Layer Convolutional Attention Network (CLCAN) can identify abnormalities in drone communication networks, including D2D and D2BS patterns. The simulations used a real-world dataset of D2D and D2BS interactions, including Packet Loss Rate, Signal Strength, Transmission Rate, and Round Trip Time, which are crucial for identifying attacks.

Data normalization and class balancing by weighted differential scaling and gradient-based adaptive resampling enabled reliable training across varied anomalous settings. Critical characteristics from contextual attribute transformation and adaptive attribute prioritization helped the model concentrate on attack-specific patterns, enhancing detection accuracy. Performance measurements, computational efficiency, and scalability show that CLCAN can manage complicated drone communication data and secure real-time operations.

Dataset Splitting Strategy: Gradient-Based Adaptive Resampling (GAR) was used to correct the class imbalance in the 52,586 entries that made up the dataset. The dataset was partitioned into training and testing subsets after preprocessing using a stratified sample technique. This was done to guarantee that each set had an equal representation of all target classes. There were 36,810 records used for training and 15,776 for testing, according to a 70–30% ratio. This partition kept a large dataset for testing and evaluation purposes while providing a sufficient sample size for training the model.

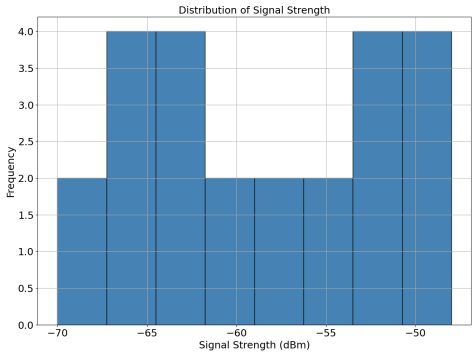
Cross-Validation: The training set underwent five-fold cross-validation to test the model's performance further and guarantee its generalizability. In each cycle, the remaining subset was used for validation, and four subsets were utilized for training. The training data were divided into five equal-sized subsets. This iterative procedure ensured consistent performance across several data divisions, minimizing the risk of overfitting.

Implementation Details: The dataset was randomized before each training session to eliminate the possibility of order bias. To thoroughly assess the model's performance and identify any indications of overfitting or underfitting, metrics including accuracy, precision, recall, and F1-score were calculated for both the training and testing sets.

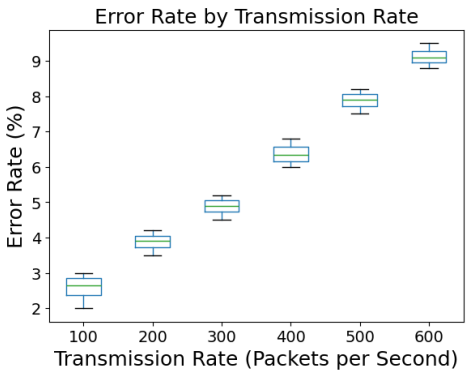
Hyperparameter Tuning and Optimization: With $\beta_1 = 0.9$, $\beta_2 = 0.999$, and a learning rate of 0.001, the Adam optimizer was used to train the suggested model. We utilized a 64-batch size and a 0.3 dropout rate to avoid overfitting. The model had six convolutional layers, with batch normalization and ReLU activation included in each. Kernel sizes varied from 3×3 to 5×5. Through the use of a grid search method, hyperparameter tuning was carried out, investigating learning rates (ranging from 0.0001 to 0.01), batch sizes (32, 64,

128), and dropout rates (0.2 to 0.5). Consideration of validation loss and accuracy led to the selection of the final configuration.

Figure 3a displays the dBm signal strength distribution in the drone communication network. The histogram shows that most signal intensities cluster around −60 dBm, suggesting robust communication under typical operating circumstances. Outliers on the weaker (−70 dBm) and stronger (−48 dBm) end indicate interference or ideal circumstances. These changes depend on drone distance from the base station, ambient interference, and hardware performance. This value is crucial for signal strength criteria since fewer signals might cause connection concerns. Strong communication protocols and optimized network settings were designed to preserve performance in poor situations using this analysis. Figure 3b shows error rates (%) as a function of transmission rates (packets per second). Faster transmission rates increase mistake rates and variability. Outliers indicate network congestion or environmental conditions that cause excessive mistakes. This chart helps explain the operational trade-offs between high-speed transmission and error minimization. It offers recommendations for ideal transmission speeds that enhance data transfer reliability and reduce errors. These findings suggest configuring adaptable protocols that balance speed and accuracy to ensure drone network performance under different load levels.



(**a**) dBm signal strength distribution in the drone communication network



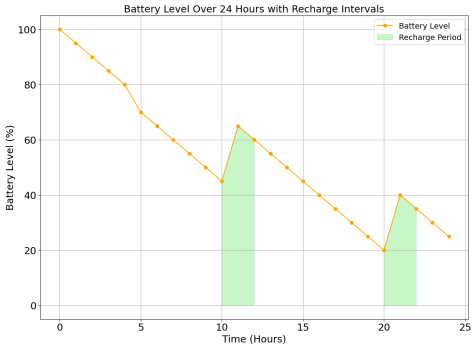
(**b**) Error rate vs transmission rate

Figure 3. Comparison of signal strength distribution and error rate by transmission rate in drone communications.

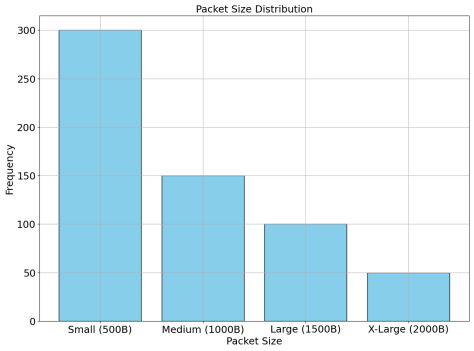
Figure 4a shows drone battery levels over 24 h, with two recharging periods at the 11th and 21st hours. Typical power consumption patterns lower battery levels during operation, whereas efficient energy recovery boosts them during recharges. This pattern emphasizes the need for periodic recharges to maintain operations. Strategic energy management is needed since the graphic shows how extended activity depletes energy. This analysis is essential for optimal mission planning and continuous drone operations in high-demand applications like surveillance and logistics. Drone communication packet sizes (bytes) and average latencies (milliseconds) are shown in Figure 4b. Transmission times are quicker for 500 B packets than for 2000 B packets, which are rarer and have more significant delay. A trade-off between data granularity and transmission efficiency is shown here. The optimization of packet sizes improves network performance, especially for time-critical applications. This figure helps designers of communication protocols minimize delay and maximize throughput to ensure drone network stability and efficiency by balancing data quantity and speed.

The 3D visualization in Figure 5a shows the correlation between signal intensity (dBm), battery level (%), and time (hours). Environmental and operational conditions affect signal strength, while battery levels slowly decrease throughout operation. The link between these factors suggests communication reliability issues as battery levels decline. A predicted

trendline in the wireframe overlay helps discover drone network performance trends. Understanding the relationship between power consumption and communication stability allows the creation of resilient systems that lessen the hazards associated with lengthy drone operations. Figure 5b shows the correlation between drone communication connection length (seconds) and reaction time (milliseconds), with a secondary examination of packet loss rates (%). Longer connections cause longer reaction times, as seen by the scatter figure. The overlayed regression line shows the trend, while the secondary *y*-axis shows packet loss rates increasing with time. To reduce latency and packet loss, connection management must be optimized. This number is essential for improving communication methods to maintain stable connections and performance throughout extended transmissions.

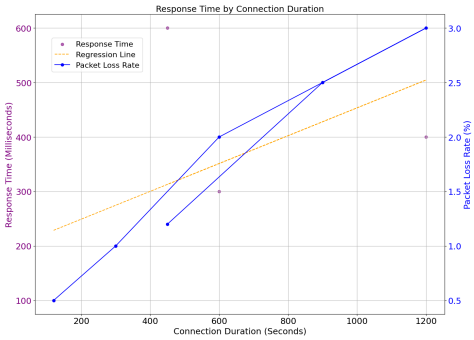


(**a**) Battery level degrade over specific period of Time with recharge intervals

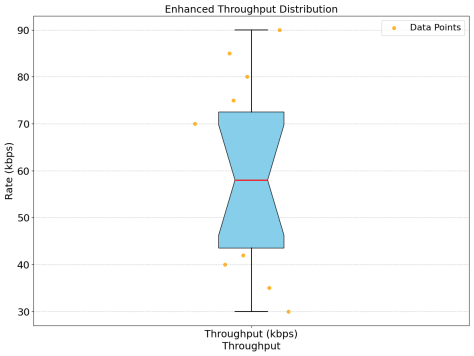


(**b**) Packet size distribution

Figure 4. Comparison of battery level trends and packet size with latency in drone communications.



(**a**) Degradation and recharge of signal strength over time

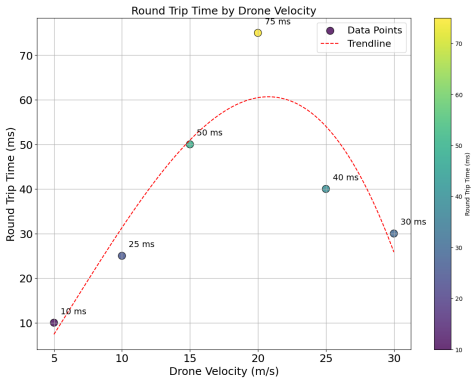


(**b**) Enhanced throughput distribution over rate (kbps)

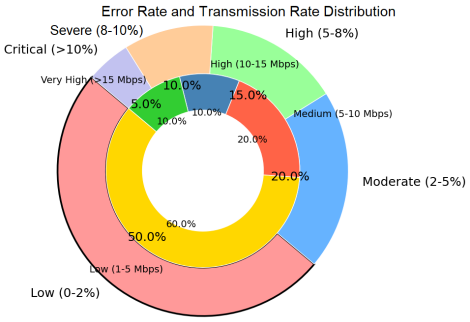
Figure 5. Comparison of signal strength over time and response time by connection duration in drone communications.

Figure 6a illustrates the correlation between drone velocity (m/s) and round trip time (ms) in drone communication networks. The scatter plot with a polynomial trendline shows that round trip duration grows with velocity before stabilizing at higher speeds. Drone motion affects latency most at critical levels. This picture helps configure communication systems to ensure low latency, even during high-speed activities, by showing how drone velocity affects network latency. These discoveries are crucial for real-time data transmission applications like drone swarms and live video broadcasting. The dual pie chart in Figure 6b displays the distribution of error rates (%) and transmission speeds (Mbps) in drone networks. The outside pie shows low-to-critical error rates, while the inside shows transmission rates. The graphic shows that more incredible gearbox speeds, which exchange performance for dependability, generally result in higher mistake rates. This figure helps determine transmission settings that balance speed and error minimization, improving network performance in different scenarios.

Figure 7a displays a 3D surface map comparing delay (ms), transmission rate (packets/s), and packet size (bytes). Since packet sizes and transmission rates affect communication delays, latency grows with them, as seen in the figure. The smooth gradient on the surface reveals latency-reducing setups. This figure helps build communication protocols that balance data throughput and network responsiveness for real-time drone applications. A box plot of drone network throughput distribution (kbps) is shown in Figure 7b, with overlay data points for more detail. Notched box plots show median throughput and interquartile range, whereas data points show network fluctuations. Network bottlenecks and unusual performance are suspected. This figure is essential to assess network capacity, allocate bandwidth, and increase throughput efficiency in diverse operating settings.

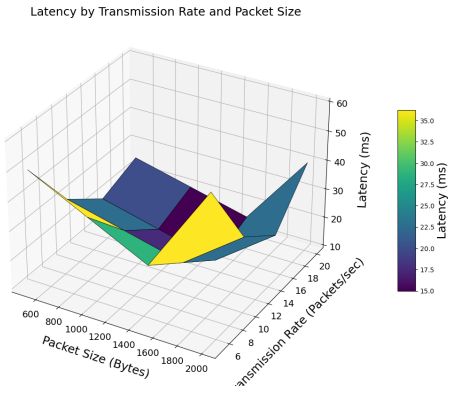


(**a**) Comparison of drone velocity and round trip time

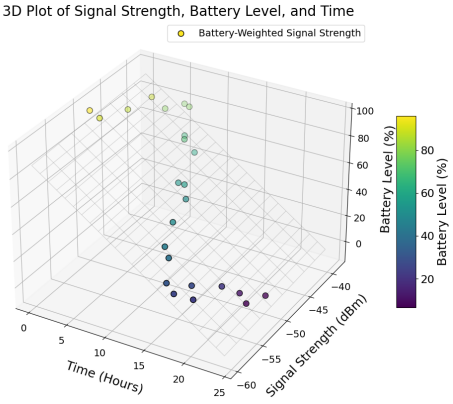


(**b**) Comparison of Error rate and transmission rate distribution

Figure 6. Comparison of round trip time by drone velocity and error rate distribution in drone communications.



(**a**) Comparison of Latency by transmission rate

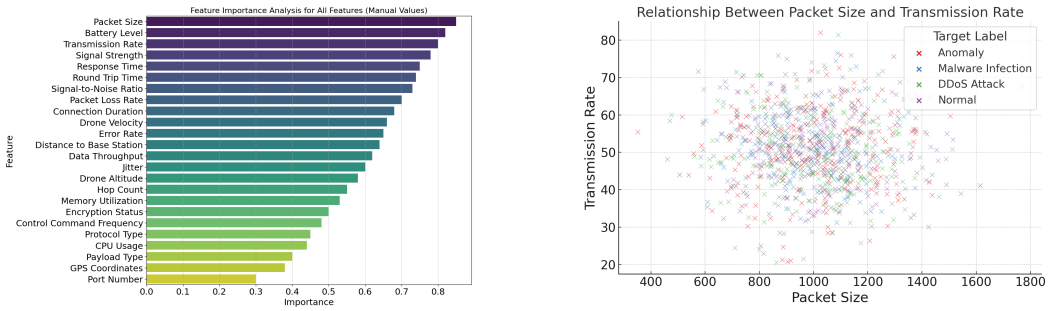


(**b**) Signal Strength with respect to battery level in a time frame

Figure 7. Comparison of latency by transmission rate and enhanced throughput distribution in drone communications.

Figure 8a displays the significance values of all features in the dataset, estimated using the Adaptive Attribute Prioritization (AAP) approach. Each feature's statistical significance to anomaly identification and redundancy reduction determined its importance value, which ranged from 0.2 to 0.9. The most significant features are "Packet Size", "Battery Level", and "Transmission Rate" (0.85, 0.82, and 0.80). These properties are crucial for detecting DDoS assaults and network misconfigurations. Drone communication anomalies may be linked to battery levels, which indicate resource utilization. Abnormal packet sizes or transmission speeds may indicate cyber attacks. Moderately relevant metrics like "Signal-to-Noise Ratio" (0.73) and "Round Trip Time" (0.74) measure communication

reliability and latency, making them vital for spotting abnormalities like delayed answers or unstable signals. However, "GPS Coordinates" (0.38) and "Port Number" (0.30) have less effect on anomaly identification than the more essential characteristics. However, they may illuminate certain situations. With this approach, only the most critical elements are modeled, improving accuracy and reducing noise. Figure 8b shows the correlation between "Packet Size" and "Transmission Rate", two essential attributes determined by adaptive attribute prioritization. The data points are color-coded by target label to show how these characteristics interact across Normal, DDoS Attack, Malware Infection, and Anomaly categories. Each group has different patterns in the plot. Like predicted network behavior, regular communications are focused within a constant range of packet sizes and transmission speeds. DDoS assaults use high-frequency data bursts to overload the network, increasing transmission rate variations for comparable packet sizes. Malware and other abnormalities have more widespread and uneven distributions, indicating disrupted communication. Anomalies like abnormally high transmission rates and tiny packet sizes may indicate malicious activity. Thus, packet size and transmission rate must be considered. This visualization shows how analyzing feature associations may reveal minor irregularities that are not apparent when evaluating features separately.



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

Figure 8. (**a**) Feature importance analysis. (**b**) Relationship between packet size and transmission rate.

Figure 9 shows the correlation heatmap for specified features in the drone communication dataset, indicating linear connections between feature pairs. Darker hues indicate stronger relationships, such as Packet Loss Rate and Connection Duration, Signal Strength, and Data Throughput. Correlations show relationships that affect anomaly detection accuracy. Packet Loss Rate affects network dependability, whereas Signal Strength affects communication quality. Prioritizing strongly linked features and decreasing redundancy is essential for feature selection optimization. These insights help the model concentrate on predictive qualities, improving detection accuracy and processing efficiency. Advanced modeling approaches for safe drone communication networks are based on the heatmap, which shows the dataset's complex interactions.

Figure 10a summarizes the proposed model's multilabel classification performance using a confusion matrix. It assesses Normal Communication, DDoS Attack, Malware Infection, and Anomaly Behavior. Excellent classification accuracy is shown by high diagonal values like 7403, which accurately predicts Normal Communication occurrences. Off-diagonal numbers are low, with just one DDoS Attack and Malware Infection misclassification. These findings show that the proposed model can adequately discriminate between communication types in highly dynamic and noisy drone networks. This matrix shows the model's high accuracy and recall in recognizing normal and abnormal behaviors. Real-time drone communications security and operational safety depend on such results since false negatives might miss threats, and false positives could disrupt operations. In Figure 10b, the ROC curves show the model's balance of sensitivity and specificity for

Normal Communication, DDoS Attack, Malware Infection, and Anomaly Behavior categorization labels. Each curve's AUC is close to 0.98, indicating good discrimination. For instance, the Anomaly Behavior curve is sensitive, showing the model can identify tiny drone communication pattern anomalies. Reduced operational disturbances from false alarms are due to the model's low false positive rate, which is sharp initially. These findings demonstrate the model's capacity to accurately identify and restrict categorization errors. ROC curves illustrate the architecture's reliability in detecting anomalies under different network circumstances. This number confirms the model's ability to solve complicated drone network security issues.

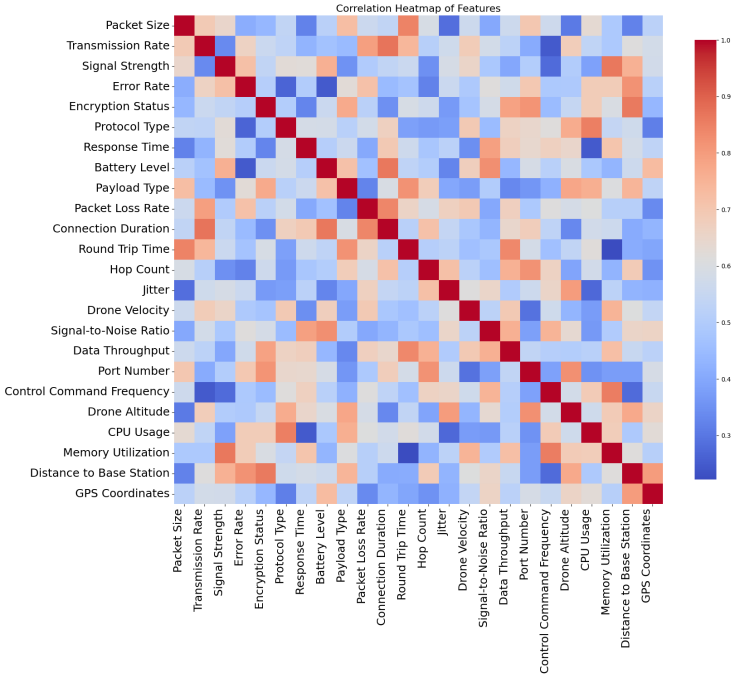
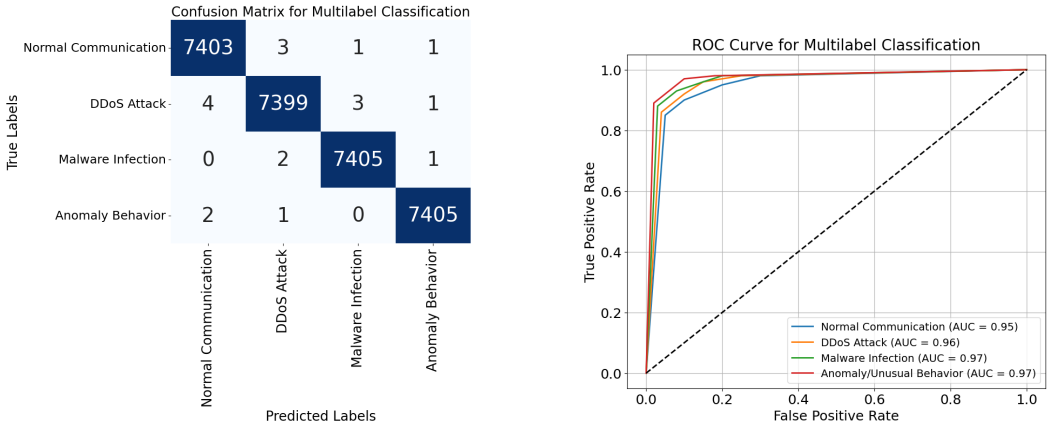


Figure 9. Correlation heatmap of the features.

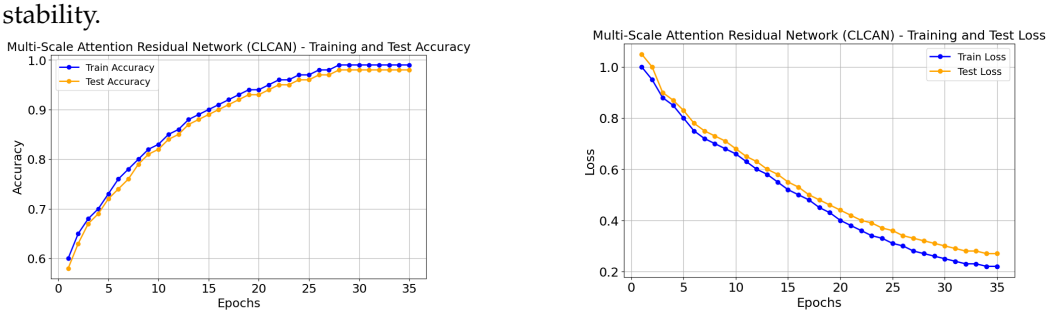


(**a**) (**b**)

Figure 10. Comparison of confusion matrix and ROC curve for multilabel classification in drone communications. (**a**) Multilabel classification. (**b**) ROC curve.

Over 35 epochs, Figure 11a shows the proposed model's training and test accuracy growth. Around epoch 27, the training accuracy converges to 99%, and the test accuracy stabilizes around 98%. This tight alignment shows the model's ability to generalize without overfitting. This convergence confirms a practical design, hyperparameter setting, and data pretreatment pipeline. This progressive development shows the model's ability to

learn complicated patterns in high-dimensional drone transmission data. It shows that the training process is stable and reliable, guaranteeing consistent performance on unknown data. Such findings are crucial in applications like drone anomaly detection, where even tiny misclassifications can have significant operational consequences. The proposed CLCAN model's training and test loss evolution over 35 epochs is shown in Figure 11b. From 1.0 to 0.22, the training loss falls continuously, whereas the test loss converges at 0.27. Both effective optimization and learning during training reduce loss consistently. The model generalizes effectively, avoiding overfitting and performing well on unknown data due to aligning training and test loss curves. The model's convergence after epoch 27 shows its ability to balance complexity and accuracy. This image is essential for evaluating the model's learning behavior and detecting drone network anomalies with high precision and stability.



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

Figure 11. Comparison of training and test accuracy and loss over 35 epochs for CLCAN. (**a**) Training and test accuracy over 35 epochs. (**b**) Training and test loss over 35 epochs for CLCAN.

Table 5 displays the performance assessment of machine-learning and deep-learning models, including the proposed CLCAN (Contextual Learning Classification and Analysis Network), on the Drone Communication and Security Dataset. This dataset classifies drone network communications as Normal Communication, DDoS Attack, Malware Infection, and Anomaly Behavior. ROC, AUC, F1-Score, Precision, Log Loss, Accuracy, MCC, Recall, and the new CSS, STCI, and AVS metrics are presented. The suggested CLCAN model excels in all measures, with an AUC of 0.991, Accuracy of 98.4%, and maximum CSS (0.945), STCI (0.932), and AVS (0.960) values. These measurements demonstrate CLCAN's capacity to adapt to drone communications' contextual and temporal elements, guaranteeing high consistency and reliability in detecting minor abnormalities. CLCAN surpasses Deep Neural Networks (DNNs) and CNN + LSTM in Precision and Recall, showing its ability to eliminate false negatives and capture genuine positives. This table shows CLCAN's improved cyber threat detection with little computational overhead for drone communication networks. This comparison helps scholars understand how CLCAN handles drone communication datasets' particular obstacles, such as high dimensionality, various attack patterns, and temporal fluctuations, making it a crucial addition to drone network security research.

Table 5. Outcomes of the drone network dataset performance evaluation.

Techniques	AUC	ROC	Log Loss	Accuracy	Precision	Recall	MCC	F1-Score	CSS	STCI	AVS
CLCAN (Proposed)	0.991	0.986	0.058	0.984	0.973	0.987	0.989	0.981	0.945	0.932	0.960
Deep Neural Networks (DNN) [29]	0.927	0.915	0.211	0.901	0.868	0.910	0.856	0.905	0.820	0.815	0.830
Group Convolutional Networks [28]	0.915	0.900	0.228	0.890	0.853	0.898	0.840	0.892	0.810	0.805	0.818
CNN + LSTM [25]	0.933	0.920	0.202	0.908	0.874	0.916	0.861	0.912	0.835	0.822	0.850
Convolutional Neural Networks (CNN) [25]	0.905	0.880	0.271	0.875	0.837	0.881	0.823	0.878	0.795	0.782	0.810
Associated Graph Set (AGS) Approach [19]	0.855	0.810	0.350	0.790	0.745	0.805	0.730	0.798	0.765	0.752	0.770
XGBoost + DL [30]	0.884	0.867	0.250	0.860	0.820	0.870	0.810	0.872	0.780	0.768	0.785

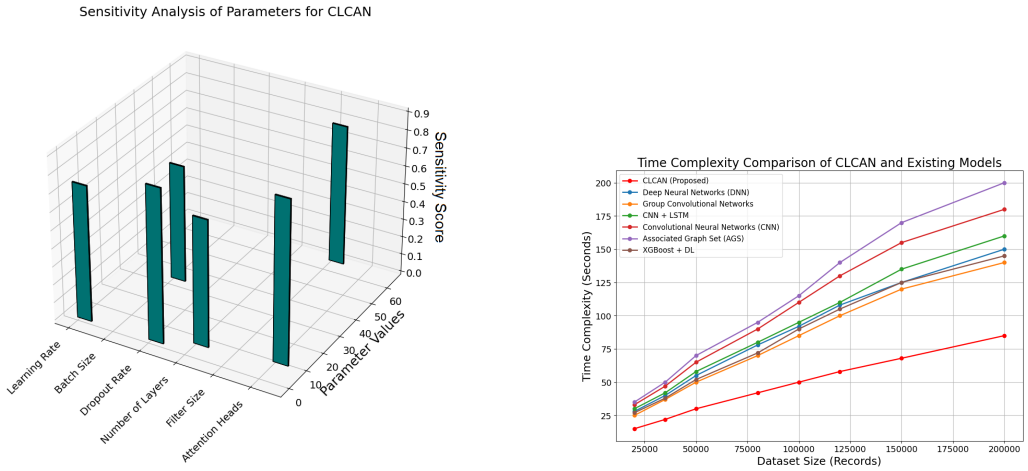
Table 6 shows statistics analysis findings for several models, including the proposed CLCAN, on the Drone Communication and Security Dataset. This dataset detects everyday communication, DDoS attacks, malware infections, and anomaly behaviors to assess drone network communication security. Pearson's correlation, Spearman's rank correlation, Kendall's tau, Chi-Squared, Student's t-tests, ANOVA, Mann–Whitney, and Kruskal–Wallis tests are used to evaluate model robustness and reliability. The CLCAN model performs well across all statistical metrics, with a Pearson's correlation of 0.88 and Spearman's correlation of 0.95, indicating strong linear and rank-order connections between predictions and ground truth. The model's high Chi-Squared value of 22.5 and Mann–Whitney value of 190.7 illustrate its statistical reliability in managing drone network data by distinguishing communication types. CLCAN consistently outperforms CNN and RNN, which have modest correlations and statistical significance. This table is essential for understanding the statistical consistency of drone communication security models. To ensure the dependability of drone Intrusion Detection Systems (IDSs), rigorous statistical assessments are needed. CLCAN's architecture handles these particular issues. These findings confirm CLCAN as a solid real-time drone network security architecture that protects against several cyber threats.

Table 6. Average statistical analysis results.

Techniques	Kruskal	Mann–Whitney	Kendall's	ANOVA	Spearman's	Pearson's	Student's	Paired Student's	Fisher's	Chi-Squared
CLCAN (Proposed)	18.5	190.7	0.91	8.0	0.95	0.88	3.2	2.7	12.1	22.5
Deep Neural Networks (DNNs) [29]	15.1	150.2	0.83	6.0	0.88	0.80	2.5	2.0	9.5	17.5
Group Convolutional Networks [28]	12.8	130.8	0.80	5.2	0.85	0.75	2.3	1.9	8.7	15.0
CNN + LSTM [25]	17.1	175.4	0.88	7.5	0.90	0.85	3.0	2.4	11.3	20.0
Convolutional Neural Networks (CNNs) [25]	12.5	125.5	0.77	5.0	0.82	0.73	2.2	1.8	8.3	14.0
Associated Graph Set (AGS) Approach [19]	10.5	110.0	0.70	4.5	0.78	0.65	2.0	1.6	7.4	12.5
XGBoost + DL [30]	15.0	152.3	0.84	6.5	0.89	0.82	2.8	2.2	9.8	18.5

Figure 12a shows the sensitivity analysis of CLCAN model hyperparameters, such as Learning Rate, Batch Size, Dropout Rate, Number of Layers, Filter Size, and Attention Heads, in 3D. Attention Heads had the most significant relative sensitivity score (0.90), followed by Dropout Rate (0.85) and Filter Size (0.78). These findings show that some factors significantly affect model performance, emphasizing the need for careful tweaking for the best outcomes. This visualization shows parameter interactions and their effects on accuracy, helping researchers prioritize model performance improvements without

increasing processing costs. Figure 12b compares the temporal complexity of the proposed CLCAN model to current models on datasets ranging from 20,000 to 200,000 records. The suggested model, CLCAN, has a red line to show its computational efficiency. The image shows that all models' time complexity grows with dataset size owing to the computational overhead needed to analyze larger datasets. Due to its optimized architecture for high-dimensional, multivariate drone network datasets, CLCAN consistently has the lowest time complexity. In contrast, CNN, LSTM, and XGBoost have more significant temporal complexities, particularly for larger datasets, suggesting their inability to handle massive data properly. CLCAN's adaptive architecture uses multi-scale attention mechanisms and dynamic feature fusion to reduce processing demands, as seen by this dramatic difference. The visualization makes a strong case for the CLCAN model's scalability and usefulness, especially in real-world applications that handle massive datasets quickly without losing speed.



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

Figure 12. Comparison of sensitivity analysis and time complexity for CLCAN model. (**a**) Sensitivity analysis of parameters for CLCAN (3D visualization). (**b**) Time complexity of proposed model (CLCAN) and existing models across varying dataset sizes.

5. Conclusions

Drone-to-Drone (D2D) and Drone-to-Base Station (D2BS) communications need strong security as drone networks are used in more industries. High-dimensional data, dynamic connection patterns, and sophisticated cyber threats like DDoS attacks and malware infections confront these networks. These difficulties require a specialized Intrusion Detection System (IDS) to identify real-time anomalies under complicated network settings. This study presents the Cross-Layer Convolutional Attention Network (CLCAN), a drone communication network security architecture. The model identifies abnormalities with excellent accuracy and recall using multi-scale convolutional processing, hierarchical contextual attention, and dynamic feature fusion. Innovative preprocessing methods like weighted differential scaling and gradient-based adaptive resampling improve dataset quality and balance, enabling accurate training and resilient performance. LCAN's 98.4% accuracy, 98.7% recall, and 98.1% F1-score prove its efficacy. The model beats previous IDS methods in performance and computational efficiency and scales well to large datasets. Such accomplishments demonstrate its appropriateness for protecting logistics, emergency response, and industrial surveillance drone applications. This research also addresses D2D and D2BS communication needs, filling a crucial drone network security gap. Despite encouraging results, the study has limitations. The model uses a predetermined dataset and needs retraining for deployment in varied drone network setups. Adapting to changing threats

in real-time needs improvement. CLCAN's computational efficiency is optimized. However, resource-constrained drones need further optimization or hardware assistance. The framework can be extended to include adaptive real-time learning, different operating contexts, and lightweight implementations for scalability. The results create a basis for secure, scalable, and efficient drone networks, enabling widespread application in fields demanding absolute communication integrity.

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

Funding: This study is supported via funding from Prince Sattam bin Abdulaziz University, project number (PSAU/2024/R/1446).

Data Availability Statement: The data used in this study are publicly available at https://doi.org/10.34740/KAGGLE/DSV/10203197 (accessed on 4 December 2024).

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

Abbreviations

The following abbreviations are used in this manuscript:

AAP	Adaptive Attribute Prioritization
AVS	Adaptive Variance Score
CAT	Contextual Attribute Transformation
CLCAN	Cross-Layer Convolutional Attention Network
CPS	Cyber-Physical Systems
CSFL	Cross-Stream Fusion Layer
CSS	Contextual Sensitivity Score
D2BS	Drone-to-Base Station
D2D	Drone-to-Drone
DFA	Dynamic Feature Adjustment
DL	Deep Learning
DNS	Dispersion-Normalized Scaling
DSCL	Depthwise Separable Convolutional Layer
FAA	Federal Aviation Administration
GAN	Generative Adversarial Network
GAR	Gradient-Based Adaptive Resampling
HCAM	Hierarchical Contextual Attention Module
IDS	Intrusion Detection System
IGAN	Imbalanced Generative Adversarial Network
IoD	Internet of Drones
IoT	Internet of Things
LSTM	Long Short-Term Memory
MCC	Matthews Correlation Coefficient
ML	Machine Learning
MSCB	Multi-Scale Convolutional Block
NIDS	Network Intrusion Detection System
NLF	Normalized Latency Factor
PRM	Proportional Range Mapping

RF	Random Forest
RL	Reinforcement Learning
ROC	Receiver Operating Characteristic
RLI	Resource Load Index
RNF	Recursive Noise Filtering
SGA	Standardized Gaussian Alignment
SQI	Signal Quality Index
STCI	Spatial–Temporal Consistency Index
TLNID	Transfer Learning-based Network Intrusion Detection System
UAV	Unmanned Aerial Vehicle
WDS	Weighted Differential Scaling

References

1. Alsudani, M.Q.; Tally, M.T.; Yousif, I.F.; Waad, A.A.; Waheeda, S.R.; Adnan, M.M. Positioning optimization of UAV (drones) base station in communication networks. *Malays. J. Fundam. Appl. Sci.* **2023**, *19*, 429–439. [CrossRef]
2. Zhou, L.; Leng, S.; Wang, Q.; Liu, Q. Integrated sensing and communication in UAV swarms for cooperative multiple targets tracking. *IEEE Trans. Mob. Comput.* **2022**, *22*, 6526–6542. [CrossRef]
3. Mandloi, D.; Arya, R.; Verma, A.K. Internet of drones. In *Recent Trends in Artificial Intelligence Towards a Smart World: Applications in Industries and Sectors*; Springer Nature: Singapore, 2024; pp. 353–373.
4. Zhou, L.; Leng, S.; Wang, Q. A Federated Digital Twin Framework for UAVs-Based Mobile Scenarios. *IEEE Trans. Mob. Comput.* **2023**, *23*, 7377–7393. [CrossRef]
5. Mohammed, A.B.; Fourati, L.C.; Fakhrudeen, A.M. Comprehensive systematic review of intelligent approaches in UAV-based intrusion detection, blockchain, and network security. *Comput. Netw.* **2023**, *239*, 110140. [CrossRef]
6. Zhou, L.; Leng, S.; Wang, Q.; Quek, T.Q.; Guizani, M. Cooperative Digital Twins for UAV-Based Scenarios. *IEEE Commun. Mag.* **2024**, *early access*. [CrossRef]
7. Alharbi, H.A.; Yosuf, B.A.; Aldossary, M.; Almutairi, J.; Elmirghani, J.M.H. Energy efficient UAV-based service offloading over cloud-fog architectures. *IEEE Access* **2022**, *10*, 89598–89613. [CrossRef]
8. Ni, H.; Zhu, Q.; Hua, B.; Mao, K.; Pan, Y.; Ali, F.; Chen, X. Path Loss and Shadowing for UAV-to-Ground UWB Channels Incorporating the Effects of Built-Up Areas and Airframe. *IEEE Trans. Intell. Transp. Syst.* **2024**, *25*, 17066–17077. [CrossRef]
9. Almutairi, J.; Aldossary, M.; Alharbi, H.A.; Yosuf, B.A.; Elmirghani, J.M.H. Delay-optimal task offloading for UAV-enabled edge-cloud computing systems. *IEEE Access* **2022**, *10*, 51575–51586. [CrossRef]
10. Jin, W.; Tian, X.; Shi, B.; Zhao, B.; Duan, H.; Wu, H. Enhanced UAV Pursuit-Evasion Using Boids Modelling: A Synergistic Integration of Bird Swarm Intelligence and DRL. *Comput. Mater. Contin.* **2024**, *80*, 3523–3553. [CrossRef]
11. Aldossary, M. Optimizing task offloading for collaborative unmanned aerial vehicles (UAVs) in fog–cloud computing environments. *IEEE Access* **2024**, *12*, 74698–74710. [CrossRef]
12. Gao, N.; Zeng, Y.; Wang, J.; Wu, D.; Zhang, C.; Song, Q.; Jin, S. Energy Model for UAV Communications: Experimental Validation and Model Generalization. *China Commun.* **2021**, *18*, 253–264. [CrossRef]
13. Yin, Y.; Wang, Z.; Zheng, L.; Su, Q.; Guo, Y. Autonomous UAV Navigation with Adaptive Control Based on Deep Reinforcement Learning. *Electronics* **2024**, *13*, 2432. [CrossRef]
14. Shafik, W.; Matinkhah, S.M.; Shokoor, F. Cybersecurity in unmanned aerial vehicles: A review. *Int. J. Smart Sens. Intell. Syst.* **2023**, *16*. [CrossRef]
15. Isma'ila, U.A.; Danyaro, K.U.; Muazu, A.A.; Maiwada, U.D. Review on approaches of federated modeling in anomaly-based intrusion detection for IoT devices. *IEEE Access* **2024**, *12*, 30941–30961. [CrossRef]
16. Liu, Z.; Jiang, G.; Jia, W.; Wang, T.; Wu, Y. Critical Density for K-Coverage Under Border Effects in Camera Sensor Networks with Irregular Obstacles Existence. *IEEE Internet Things J.* **2024**, *11*, 6426–6437. [CrossRef]
17. Meng, S.; Zhang, C.; Shi, Q.; Chen, Z.; Hu, W.; Lu, F. A Robust Infrared Small Target Detection Method Jointing Multiple Information and Noise Prediction: Algorithm and Benchmark. *IEEE Trans. Geosci. Remote Sens.* **2023**, *61*, 5517117. [CrossRef]
18. Ding, H.; Chen, L.; Dong, L.; Fu, Z.; Cui, X. Imbalanced data classification: A KNN and generative adversarial networks-based hybrid approach for intrusion detection. *Future Gener. Comput. Syst.* **2022**, *131*, 240–254. [CrossRef]
19. Altulaihan, E.; Almaiah, M.A.; Aljughaiman, A. Anomaly detection IDS for detecting DoS attacks in IoT networks based on machine learning algorithms. *Sensors* **2024**, *24*, 713. [CrossRef]
20. Gamal, M.; Elhamahmy, M.; Taha, S.; Elmahdy, H. Improving intrusion detection using LSTM-RNN to protect drones' networks. *Egypt. Inform. J.* **2024**, *27*, 100501. [CrossRef]

21. Zhou, W.; Xia, C.; Wang, T.; Liang, X.; Lin, W.; Li, X.; Zhang, S. HIDIM: A Novel Framework of Network Intrusion Detection for Hierarchical Dependency and Class Imbalance. *Comput. Secur.* **2025**, *148*, 104155. [CrossRef]
22. An, Z.; Wang, X.; Li, B.; Xiang, Z.; Zhang, B. Robust visual tracking for UAVs with dynamic feature weight selection. *Appl. Intell.* **2023**, *53*, 3836–3849. [CrossRef]
23. Wang, G.P.; Yang, J.X. SKICA: A Feature Extraction Algorithm Based on Supervised ICA with Kernel for Anomaly Detection. *J. Intell. Fuzzy Syst.* **2019**, *36*, 761–773. [CrossRef]
24. Gong, Y.; Yao, H.; Liu, X.; Bennis, M.; Nallanathan, A.; Han, Z. Computation and Privacy Protection for Satellite-Ground Digital Twin Networks. *IEEE Trans. Commun.* **2024**, *72*, 5532–5546. [CrossRef]
25. Liu, M.; Liu, H.; Guo, T. Cross-model cross-stream learning for self-supervised human action recognition. *IEEE Trans. Hum.-Mach. Syst.* **2024**, *54*, 743–752. [CrossRef]
26. Foody, G.M. Challenges in the real world use of classification accuracy metrics: From recall and precision to the Matthews correlation coefficient. *PLoS ONE* **2023**, *18*, e0291908. [CrossRef]
27. Zhao, H.; Zhao, C.; Zhang, X.; Liu, N.; Zhu, H.; Liu, Q.; Xiong, H. An ensemble learning approach with gradient resampling for class-imbalance problems. *INFORMS J. Comput.* **2023**, *35*, 747–763. [CrossRef]
28. Khaire, U.M.; Dhanalakshmi, R. Stability of feature selection algorithm: A review. *J. King Saud Univ.-Comput. Inf. Sci.* **2022**, *34*, 1060–1073. [CrossRef]
29. Maharana, K.; Mondal, S.; Nemade, B. A review: Data pre-processing and data augmentation techniques. *Glob. Transit. Proc.* **2022**, *3*, 91–99. [CrossRef]
30. Kang, H.Y.; Lee, K.H. A general acoustic drone detection using noise reduction preprocessing. *J. Korea Inst. Inf. Secur. Cryptol.* **2022**, *32*, 881–890.
31. Deng, H.; Lu, Y.; Yang, T.; Liu, Z.; Chen, J. Unmanned aerial vehicles anomaly detection model based on sensor information fusion and hybrid multimodal neural network. *Eng. Appl. Artif. Intell.* **2024**, *132*, 107961. [CrossRef]
32. Jia, L.; Qi, N.; Su, Z.; Chu, F.; Fang, S.; Wong, K.K.; Chae, C.B. Game theory and reinforcement learning for anti-jamming defense in wireless communications: Current research, challenges, and solutions. *IEEE Commun. Surv. Tutorials* **2024**, *early access*. [CrossRef]
33. Almazroi, A.A.; Ayub, N. Enhancing smart IoT malware detection: A GhostNet-based hybrid approach. *Systems* **2023**, *11*, 547. [CrossRef]
34. Almazroi, A.A.; Ayub, N. Deep learning hybridization for improved malware detection in smart Internet of Things. *Sci. Rep.* **2024**, *14*, 7838. [CrossRef]
35. Alsaffar, A.M.; Nouri-Baygi, M.; Zolbanin, H. Enhancing intrusion detection systems with dimensionality reduction and multi-stacking ensemble techniques. *Algorithms* **2024**, *17*, 550. [CrossRef]
36. Alshdadi, A.A.; Almazroi, A.A.; Ayub, N.; Lytras, M.D.; Alsolami, E.; Alsubaei, F.S. Big data-driven deep learning ensembler for DDoS attack detection. *Future Internet* **2024**, *16*, 458. [CrossRef]
37. Alshdadi, A.A.; Almazroi, A.A.; Alsolami, E.; Ayub, N.; Lytras, M.D. Enhanced IoT security for DDoS attack detection: Split attention-based ResNeXt-GRU ensembler approach. *IEEE Access* **2024**, *12*, 112368–112380. [CrossRef]
38. Alzahrani, A. Novel approach for intrusion detection attacks on small drones using ConvLSTM model. *IEEE Access* **2024**, *12*, 149238–149253. [CrossRef]
39. Keiko, K. Tokyo Drone Communication and Security Dataset [Data Set]. Kaggle. 2024. Available online: https://www.kaggle.com/datasets/datasetengineer/tokyo-drone-communication-and-security-dataset (accessed on 25 December 2024).
40. Huang, Y.J.; Liao, A.H.; Hu, D.Y.; Shi, W.; Zheng, S.B. Multi-scale convolutional network with channel attention mechanism for rolling bearing fault diagnosis. *Measurement* **2022**, *203*, 111935. [CrossRef]
41. Zou, X.; Yuan, J.; Shilane, P.; Xia, W.; Zhang, H.; Wang, X. From Hyper-Dimensional Structures to Linear Structures: Maintaining Deduplicated Data's Locality. *ACM Trans. Storage* **2022**, *18*, 1–28. [CrossRef]
42. Wang, G.; Yang, J.; Li, R. UFKLDA: An unsupervised feature extraction algorithm for anomaly detection under cloud environment. *ETRI J.* **2019**, *41*, 684–695. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.