Received: 22 September 2025 | Revised: 25 November 2025 | Accepted: 6 January 2026 | Published online: 21 August 2026

RESEARCH ARTICLE

Journal of Computational and Cognitive Engineering
2026, Vol. 00(00) 1–13
DOI: 10.47852/bonviewJCCE62027734

BON VIEW PUBLISHING

From Telemetry to Trust: A Lightweight Statistical–Spectral LSTM Framework for UAV Anomaly-Based IDS

Hafiz Muhammad Attaullah[1], Inam Ullah Khan[1], Thabit Mahmood Thabit[1], Muhammad Mansoor Alam[1,2] and Mazliham Mohd Su'ud[1,*]

[1] *Faculty of Computing and Informatics, Multimedia University, Malaysia*

[2] *Faculty of Computing, Riphah International University, Pakistan*

Abstract: Unmanned aerial vehicles (UAVs) in mission-critical applications are subjected to advanced cyberattacks of UAV-specific protocols and sensor streams, necessitating intrusion detection systems (IDS) that are sensitive to tight energy constraints and low-latency constraints on airborne edge systems. Current UAV IDS face a critical accuracy–efficiency trade-off: high-accuracy deep learning models exceed the computational capabilities of airborne edge platforms, while lightweight approaches fail to detect sophisticated attacks. This work introduces a novel Long Short-Term Memory (LSTM)-based framework that combines systematic multi-modal feature engineering with compact temporal modeling for resource-constrained UAV deployment. Our solution presents the Windowed Statistical–Spectral (WSS-64) Framework, a multi-modal feature intelligence system that ingests raw UAV telemetry and network traces and runs a 2 Hz compact LSTM model that converts these traces into 64-dimensional frames to provide consistent and accurate detection of classical cyberattacks, including spoofing, false data injection, and denial-of-service malfunctions. Our systematic combination of statistical, spectral, and network characteristics into fixed-dimensional representations optimized for a time model with resource constraints is the main novelty. The method yields a macro-F1 of 0.992 and an AUROC of 0.9995 with 99.21% accuracy and false positive (0.8%) and false negative (0.9%) rates, significantly higher than baseline methods such as Decision Tree (94.85%), Random Forest (96.32%), Support Vector Machine (95.10%), and Convolutional Neural Network (97.45%). The WSS-64 Framework offers O(N) linear complexity for real-time UAV operations.

Keywords: UAV security, intrusion detection, anomaly detection, edge computing, cyber-physical systems

1. Introduction

Unmanned aerial vehicles (UAVs) have emerged as essential resources in mission-critical tasks such as surveillance operations, emergency response management, logistics and supply chain management, and autonomous delivery systems in which operational failure may lead to major economic damage, jeopardized public security, or even mission failure with a ripple effect [1]. The rising scale of UAV activity operations, whether at the level of single units or at the level of autonomous service of fleets, has opened an attack surface on an unprecedented level, which is actively being used by advanced attackers through specific cyberattacks [2].

UAV security space involves various attack vectors that include physical layer noise, manipulation of communication protocols, control system manipulation, and application vulnerability. Current studies prove that critical UAV weaknesses such as GPS spoofing attacks and jamming attacks undermine the accuracy of navigation [3], attacks on UAV communications that interfere with inter-system coordination are protocol-specific [4], and network-based attacks including Wi-Fi deauthentication and evil-twin attacks that compromise command and control channels [5]. Advanced adversarial methods use detection systems on UAVs by taking advantage of advanced machine learning methods aimed at defeating traditional security protocols [6], while comprehensive vulnerability assessments reveal systematic weaknesses across commercial drone platforms [2]. By using Radio Frequency (RF) jamming, GPS spoofing, and communication link disruption, electronic warfare capabilities that target UAV avionics systems pose additional difficulties that could seriously jeopardize autonomous operations [7].

The basic trade-off between detection accuracy and computational efficiency needed for edge deployment is not addressed by current intrusion detection systems (IDS), despite a great deal of research in UAV security. The operation of the UAV IDS has specific limitations, which make them unlike conventional network or host-based security systems. Airborne edge hardware has tight energy constraints in which the computational overhead of a mission has a direct relationship with flight time and flight range, and low-latency requirements require threat

***Corresponding author:** Mazliham Mohd Su'ud, Faculty of Computing and Informatics, Multimedia University, Malaysia. Email: mazliham@mmu.edu.my

detection in real time without disrupting flight control response [1]. The existing methods of intrusion detection have a fundamental accuracy–efficiency trade-off: high-accuracy deep learning models are expensive in terms of both computational resources and power consumption, well beyond the capabilities of most UAV platforms, whereas lightweight designs do not provide as high-quality detection but do not attempt to identify more sophisticated attack patterns that target specific UAV-focused protocols and sensor data streams [8]. A thorough review of the literature shows important problems that make it impossible to use UAV IDS in real life. Ogab et al. [9] conducted a systematic review of 62 Internet of Drones IDS papers, finding that network-based approaches are prevalent, with LSTM/CNN/Autoencoder families commonly employed, but datasets are often outdated or non-UAV-specific, with limited consideration of UAV operational constraints. Complex deep learning models without comprehensive latency or energy consumption analysis prove impractical for resource-constrained UAV platforms [8]. While energy-efficient approaches show promise in Internet of Things (IoT) environments [10] and resource-constrained systems [11], they require significant adaptation for UAV-specific constraints including cross-sensor validation requirements and temporal correlation analysis. The previous studies lack a unified framework that (1) combines statistical, spectral, and network features from synchronized multi-modal UAV data, (2) achieves high detection accuracy with O(N) linear complexity suitable for edge deployment, and (3) validates on UAV-specific datasets with diverse attack types.

In this work, we present the Windowed Statistical–Spectral (WSS-64) Framework, a unified and lightweight intrusion detection approach tailored for UAVs. Our approach is a systematic combination of statistical characteristics, spectral features, and side network intelligence into small 64-dimensional representations that can be easily deployed at the edges. These sequences are then processed with a compact Long Short-Term Memory (LSTM) classifier that makes sure to detect the anomalies accurately in a latency and energy-efficient manner that is highly constrained in terms of resources. LSTM networks are particularly suited for UAV intrusion detection due to their ability to model temporal dependencies in sequential telemetry data. Unlike feedforward networks, LSTMs maintain memory of past states, enabling detection of time-evolving attack patterns that manifest across multiple time steps in UAV sensor streams and network traffic [4, 8]. The WSS-64 Framework addresses real-world UAV operational constraints by providing fixed 64-dimensional representations with O(N) linear complexity and predictable memory footprint, enabling deployment on resource-constrained edge hardware without compromising flight time or mission range, critical factors for autonomous surveillance, emergency response, and delivery operations.

Key contributions are as follows:

1) WSS-64 Feature Engineering: Edge-friendly representation WSS features in 64-D vectors at 2 Hz, uniquely integrating statistical, spectral, and network intelligence from synchronized telemetry and network traces with O(N) linear complexity.
2) Lightweight LSTM: Small recurrent dropout and dense head network that is optimized to achieve low-latency UAV detection, achieving 1.71% improvement over raw LSTM while maintaining computational efficiency.
3) Multi-Modal Fusion: Combined application of UAV telemetry and network traces in detecting spoofing, false data injection (FDI), and denial-of-service (DoS) attacks, providing inherent robustness as adversaries must simultaneously compromise multiple independent data channels.
4) Efficiency: Linear-time complexity with fixed memory, supporting the UAV operations under energy constraints.

This paper's remaining sections are arranged as follows: Section 2 examines relevant research. The proposed framework is presented in Section 3. The experimental setup is explained in Section 4. Results are presented and discussed in Section 5. Section 6 brings the paper to a close.

2. Related Work

The modern state of the UAV and IoT intrusion detection research covers a wide variety of methodological and application fields of the research, which, nevertheless, provide certain insights and demonstrate certain limitations in the real practice of their implementation [12]. UAV environment IDS can be qualitatively grouped into three main strategies depending on their detection processing and the computational basis [12]. Rule-based or signature-based IDS systems compare known attack instances to known signatures that are built based on previously identified threat indicators and malicious patterns of behavior and offer high specificity to known threats but low ability to detect new ones. Classical algorithms used in machine learning–based IDS solutions include Support Vector Machines, Random Forests, and k-Nearest Neighbors on engineered features based on the UAV telemetry and network traffic [11], providing better generalization properties than rule-based systems and being interpretable and computationally efficient enough to be used in resource-constrained environments. Deep learning-based IDS uses neural network models such as Convolutional Neural Networks (CNNs), LSTM networks, and autoencoders to raw signals or sequences of features [8], delivering advanced pattern recognition features that are capable of finding complicated temporal associations and nonlinear correlations in UAV operational data. Du et al. [4] developed a UGL hybrid GCN+LSTM approach achieving 100% flooding attack detection and 98.54% fuzzy attack detection on UAVCAN datasets through graph-based temporal modeling, demonstrating the effectiveness of combining graph neural networks with recurrent architectures for protocol-specific attacks. Hadi et al. [5] introduced the UAV-NIDD dataset with Feedforward Neural Networks achieving 99.02% accuracy on Wi-Fi-based attacks, focusing on real-time UAV network traffic analysis across UAV/AP/GCS scenarios and providing the first comprehensive multi-scenario UAV network dataset. Wang et al. [8] proposed TBCLNN using Progressive Self-Knowledge Distillation achieving 99.71% accuracy with only 4.6K parameters and 17.8KB model size, demonstrating lightweight model feasibility for IoT environments through advanced knowledge distillation techniques. Yoo et al. [3] developed MeNU memory-augmented autoencoder achieving 0.9856/0.9988 Area Under the Curve (AUC) on ALFA and UA datasets for GPS spoofing/jamming detection using unsupervised learning approaches that maintain memory banks of normal operational patterns. Alzubaidi [13] introduced RPCA-Net for UAV flight anomaly detection achieving 94.02% F1-score on engine failure detection using reconstruction–prediction co-learning attention networks that combine temporal modeling with anomaly reconstruction. Several recent studies highlight progress in lightweight and edge-suitable IDS solutions. Aljabri et al. [14] proposed DMLP with

dynamic entropy features, enabling ultra-lightweight CAN intrusion detection. Jamshidi et al. [10] presented EIDM for Software-Defined Networking (SDN)/IoT networks with detailed resource profiling. Zeng and Nait-Abdesselam [15] combined CTGAN with human-in-the-loop learning to reduce labeling effort, while Kushwaha et al. [11] achieved resource-efficient feature selection using mFCBF with LightGBM/XGBoost. Nandanwar and Katarya [16] introduced Cyber-Sentinet with explainability support via SHapley Additive exPlanations (SHAP), and further works [17, 18] explored energy optimization and feature selection for constrained IoMT environments. In Reference [19], the authors proposed a periodic deep reinforcement learning–based lightweight Intrusion Detection and Prevention System (IDPS) for UAV networks, demonstrating autonomous attack detection with consideration for energy consumption and periodic offline learning, though their approach focuses on reinforcement learning rather than multi-modal feature engineering. Zhang [20] introduced TinyML-based lightweight models achieving 98.7% authentication accuracy and 1.2MB model size for UAV identity authentication, emphasizing edge deployment through pruning and quantization techniques. Wang et al. [21] presented a feature-based edge intelligence framework for real-time foreign object detection with optimized deployment on NVIDIA Jetson devices, highlighting the importance of edge-optimized architectures for practical deployment scenarios. Vision-based techniques have also been considered in the UAV field, such as anomaly detection [22, 23], crowd analysis [24], and formation control under DoS attacks [25]. Other efforts focused on adversarial robustness [6] and lightweight detection with YOLO-based models [26]. The issue of adversarial robustness is also essential and can be addressed by more advanced attackers evading detection by the usage of adversarially perturbed inputs [27]. Adaptive adversaries that take advantage of model vulnerabilities must be taken into account by IDS in addition to nominal attack patterns [28]. By combining various data sources, our multi-modal feature fusion in the WSS-64 Framework adds inherent robustness and makes it more difficult for adversaries to simultaneously manipulate all feature channels undetected. Survey analyses underscore gaps in UAV-specific IDS; for example, Zhou et al. [12] noted that network signatures often fail to capture UAV attack patterns, while Ogab et al. [9] reviewed 62 IoD-IDS papers and found limited availability of UAV-specific datasets. Additional perspectives include moving-target defense in SDN [28] and edge-focused deep learning frameworks [29], further emphasizing the need for tailored, efficient UAV IDS solutions. Recent advances in machine learning–based authentication [30] and unsupervised feature selection [31] show how intelligent security measures can be applied more broadly, while comprehensive surveys [32, 33] draw attention to the significance of integrating machine learning and behavioral analytics for the protection of critical infrastructure, which are concepts that guide our multi-modal approach to UAV security. Table 1 presents a comprehensive comparative analysis of existing UAV IDS approaches, highlighting their computational complexity characteristics and deployment feasibility.

Table 1
Comparative analysis of UAV IDS approaches: computational complexity and deployment feasibility

Study	Dataset	Method	UAV-specific	Lightweight	Performance	Key limitations
[4]	UAVCAN attack	GCN+LSTM	Yes	$O(n^2)$ complexity	99.9% flooding, 98.54% fuzzy, 96.35% replay	Weaker replay detection; no deployment metrics
[5]	UAV-NIDD	FNN	Yes	Cloud-based	99.02% accuracy	Limited to Wi-Fi; no per-class metrics
[8]	IoT datasets	TBCLNN	No	Yes (4.6K params, 17.8 KB)	99.71% accuracy	Non-UAV evaluation; general datasets
[3]	ALFA, UA	MemAE	Yes	Memory-intensive	0.9856/0.9988 AUC	Unsupervised only; limited attack types
[13]	ALFA	RPCA-Net	Yes	No (8.03M params)	94.02% F1-score	Heavy architecture; flight anomalies only
[14]	CAN datasets	DMLP	No	Yes (0.17 ms inference)	0.9995 F1-score	Automotive focus; not UAV-specific
[10]	CICIDS2017	EIDM	No	Yes (energy profiled)	99.56% accuracy	Network-only; no UAV threats
[15]	CIC-IDS2017, UNSW-NB15	CTGAN+HITL	No	Variable complexity	99.16% accuracy	General datasets; no UAV evaluation
[11]	CICIDS 2017, NSL-KDD, BoT-IoT	mFCBF+LightGBM	No	Yes (2.03% CPU, 1.2% memory)	99.75% accuracy	Static feature selection; no UAV data
[16]	Edge-IIoT-2022	CNN+ResNet	No	Complex architecture	97.46% accuracy	CPS focus; limited UAV applicability

In this analysis, it can be seen that the majority of the current approaches trade detection accuracy for computational efficiency or accuracy on deployment feasibility. Graph-based methods such as UGL are $O(n^2)$ and impractical in real-time UAV requirements, and heavy architectures such as RPCA-Net with 8.03M parameters surpass edge hardware. The lightweight models like TBCLNN are feasible, yet they are not evaluated on UAV specifically, whereas the memory-intensive models like MemAE have predictable variable resource usage. This gap then needs to be bridged uniquely by ensuring that the accuracy and O(N) linear complexity are maintained by carefully systematic multi-modal feature engineering as opposed to complex architectural designs. The analysis identifies serious gaps in current solutions, especially when it comes to UAV-specific analysis and lightweight implementation factors that our WSS-64 Framework will cover.

The literature also indicates a basic trade-off between engineered properties and end-to-end deep learning solutions to IDS design, with both methodologies having respective benefits and limitations to UAV deployment case scenarios [11]. Strong accuracy (≥99.3%) with extremely low usage of resources on IoT benchmarks with feature-based methods like mFCBF with boosted trees can mean that well-designed domain-specific features can provide discriminative power at computational efficiency with O(N) linear complexity versus $O(n^2)$ or $O(n^3)$ complexity of deep graph neural networks. In our WSS-64 Framework, this trade-off is particularly considered by ensuring O(N) linear complexity of computation and higher accuracy with systematic multi-modal feature engineering [11]. Computational limitations and energy efficiency are the determining factors to apply UAV IDS since autonomous aerial platforms are run within stringent power specifications and processing limits that directly affect mission duration and operating capacity [10]. Energy-conscious IDS evaluation demonstrates that, given a set of conditions, deep learning methods can be more energy-efficient than classical baselines [10], especially when the complexity of the model is balanced well with the performance of detection requirements. Nonetheless, the majority of current energy-conscious research is on generic IoT situations with nondeterministic, constantly changing dimensions and uncertain memory requirements instead of UAV-specific constraints necessitating deterministic fixed-dimensional representations and predictable computation cost when deploying edge-based computations in real-time.

3. Methodology

The WSS-64 Framework is based on a linear end-to-end workflow to process UAV telemetry and network data using a series of combined steps, starting with raw data collection via deployed edge inference features with real-time threat detection opportunities. The entire system architecture is presented in Figure 1, with the data flow running through the interface of the collection system up to the data center WSS-64 feature intelligence system until the ultimate IDS alerts and interpretability units. The end-to-end pipeline reflects how we are going to integrate data processing of multi-modal UAV security data by considering edge deployment optimization.

The WSS-64 Framework architecture demonstrates the complete pipeline from data collection to edge deployment with IDS alerts and interpretability components. The workflow begins with synchronized UAV datasets containing telemetry data (GPS, IMU, barometer, flight control parameters) and network traces (communication logs, packet captures, protocol analysis). The core WSS-64 Feature Intelligence System implements our algorithmic approach to extract unified statistical, spectral, and network features with a fixed 64-dimensional output suitable for predictable edge deployment. The Learning Module incorporates our compact LSTM architecture with 64-hidden state dimensions optimized for temporal sequence processing under computational constraints. The Windowed Statistical–Spectral (WSS) Feature Engineering and Sequence Construction algorithm is the fundamental innovation of our system that converts raw UAV data into feature representations that are structured 64-dimensional and optimized to be represented in terms of time and asserted at the edges of data. Algorithm 1 takes synchronized telemetry and network traces and uses sliding windows to do so in order to compute multi-modal feature sets that are both comprehensive and have O(N) linear computational complexity and a predictable memory footprint.

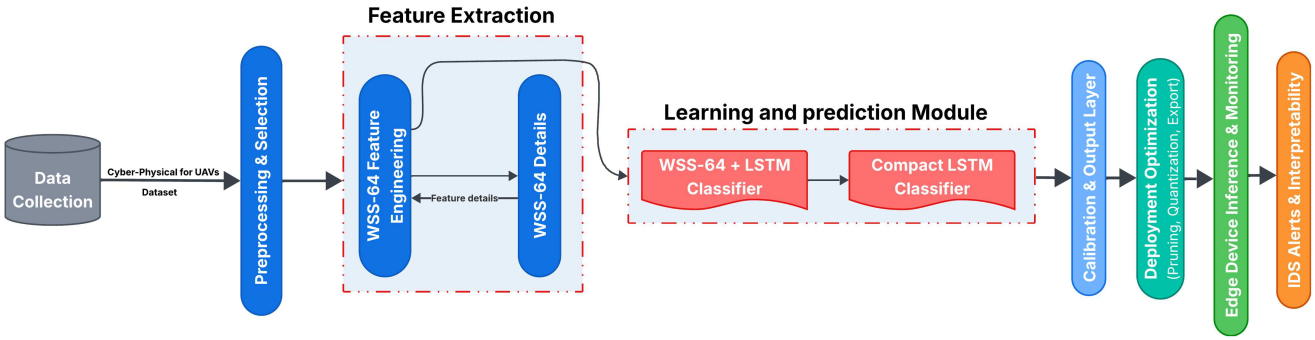
Algorithm 1: Windowed Statistical–Spectral Feature Engineering and Sequence Construction

Require: Benchmarked dataset D with synchronized telemetry $S(t)$ and network traces $N(t)$; window $W = 2$s; stride $s = 0.5$s; sub-window $w_{sub} \in \{0.25, 0.5\}$s

Ensure: Per-sample sequences $F_i \in \mathbb{R}^{T\times 64}$; fitted scaler Θ_{scal}; PCA params Θ_{PCA}; feature spec Φ

1: **0. Synchronization and Cleaning**
2: Resample all channels to a common rate; forward-fill small gaps; remove spikes via median filter
3: **1. Sliding Windowing**
4: **for** each recording $x \in D$

Figure 1
WSS-64 Framework architecture



5: Slide window of length W with stride s to obtain windows $\{x_k\}$ aligned across all channels
6: **end for**
7: **2. Per-Window Feature Blocks**
8: **for** each window x_k
9: **(a) Statistical features** for each scalar channel c:
10: Compute {mean, std, min, max, Interquartile Range (IQR), Root Mean Square (RMS), skew, kurt} on $x^{(c)}$
11: Compute temporal deltas $\Delta x^{(c)}$ stats and zero-crossing rate Zero-Crossing Rate (ZCR)
12: **(b) Spectral features** per c (using sub-windows of length w_{sub}):
13: Apply Hamming window; FFT → PSD. For bands $b \in B$, compute bandpower P_b; compute spectral entropy H_s
14: **(c) Network-traffic features** (if $N(t)$ available):
15: Packet rate (pps), inter-arrival mean/std, flow duration, SYN/ACK ratio, retransmission rate
16: Concatenate all features into a raw vector f_{raw_k} with feature list Φ
17: **end for**
18: **3. Robust Scaling**
19: Split D into train/val/test by recording. Fit RobustScaler on train: for each feature j, store (m_j = median, q_j = IQR) as Θ_{scal}
20: Scale all windows: $f_{sc_{k,j}} = (f_{raw_{k,j}} - m_j)/q_j$
21: **4. Dimensionality Reduction to 64-D**
22: Fit PCA on train features to retain 95–98% variance, capped at $d = 64 \Rightarrow \Theta_{PCA}$
23: Transform each window to $z_k \in \mathbb{R}^{64}$
24: **5. Sequence Building**
25: Group consecutive frames belonging to the same flight segment to form $F_i = [z_k, z_{k+1}, \dots] \in \mathbb{R}^{T\times 64}$ at 2 Hz
26: **return** $\{F_i\}$, Θ_{scal}, Θ_{PCA}, Φ

The systematic method guarantees the same feature extraction in a wide range of UAV operational conditions and computational efficiency that is needed to implement edge deployment in real-time. The WSS-64 Feature Intelligence System has a number of innovations involved in the deployment of UAVs. GPS-IMU correlation checks are part of the cross-sensor validation process to identify inconsistencies that could be due to a spoofing attack, and temporal delta analysis is used to identify a rapid variation, which could be the start of an attack. The spectral analysis with bands, $B = \{[0,2],\ [2,5],\ [5,10]\}$ Hz, in particular, targets the frequency of the UAV control and the communication protocols. The 64-dimensional fixed output guarantees a predictable memory consumption and a computational overhead necessary to fit an architecture at the edge, whereas the 2 Hz sampling rate maximizes the trade-off between the latency of attack detection and the cost of using the architecture.

The dimensionality reduction technique, which is called Principal Component Analysis (PCA) (that we are using), is a compromise between computational efficiency and feature preservation. Whereas UAV telemetry is nonlinear, PCA has deterministic, rapid transformations (O(d^{2}n) complexity) that can be used in real-time upon edge deployment with constant memory demands. Nonlinear models like autoencoders, albeit having the ability to represent complex manifolds, have variable computational costs (based on the depth of the network structure and the final convergence of the training) and unpredictable memory requirements that cannot fit within the hard resource limits of a UAV. Linear transformation of PCA allows effective on-device inference using previously computed projection matrices, which guarantees predictable latency that is vital when safety-critical UAVs are used. The analysis of the computational complexity shows that the feature extraction method of WSS-64 has O(N) linear complexity, where N is the total length of the sequence, O(W) operations per window, and O(W log W) spectral analysis through FFT. Compared to graph-based approaches with O(n^2) edge computation and message passing, our linear complexity reduces computational burden by orders of magnitude for real-time UAV scenarios. Empirically, feature extraction for a 2-s window requires O(10^3) operations versus O(10^6) for graph neural network approaches with 100 nodes, demonstrating substantial efficiency gains. The fixed 64-dimensional output further guarantees constant memory allocation (O(1) per frame), unlike variable-size graph representations or attention mechanisms requiring O(T^2) memory for sequence length T. This is much better than graph-based methods that have O(n^2) complexity and more memory-intensive autoencoders that need memory banks storing their variables. The Training algorithm builds the specifics of the LSTM classifier, which is a compact classifier, and optimizes it for UAV anomaly detection that is constrained by edges. The training algorithm, Algorithm 2, is an optimized neural network architecture, which is developed to handle variable-length sequences with masked input processing, recurrent layers with dropout regularization, and a classification head that is optimized to detect multi-clusters of attacks without losing computational efficiency. The edge-based design guarantees the predictable use of resources that can be deployed to real-time UAV missions in difficult situations of computational and energy limitations. The small LSTM design has a number of edge deployment optimization strategies. The fixed dimension of 64 hidden states balances the model expressiveness and the computation constraints, whereas the simplified two-layer structure eliminates overfitting on small datasets of UAV attacks. The O($T \times h^2$)forward pass time with memory needs of O($h + T \times h$) to store the hidden state implies predictable resource use that could be applied in real-time UAV work. The framework deployment pipeline integrates seamlessly through Calibration and Output Layer for threshold optimization, Deployment Optimization for pruning/quantization/export transformations, Edge Device Inference and Monitoring for real-time operation, and IDS Alerts and Interpretability for actionable security notifications. This comprehensive approach ensures that the WSS-64 Framework can be practically deployed on UAV edge hardware while maintaining superior detection performance.

Algorithm 2: Training: Construct and Optimize the WSS-64 + LSTM Classifier Construction

Require: Sequences $\{F_i \in \mathbb{R}^{T_i\times 64}\}$; labels $y_i \in$ {Normal, Spoofing, FDI, DoS}; class weights w; hyperparams (hidden size $h = 64$, layers $L \in \{1, 2\}$, dropout $p = 0.2$, bidirectional flag)

Ensure: Trained parameters Θ_{LSTM}

1: **1. Model Definition**
2: Input layer with masking (pads to max T)
3: Optional LayerNorm on inputs; input dropout p
4: Stack L LSTM layers (hidden size h); use recurrent dropout p
5: If bidirectional: concatenate forward/backward hidden states
6: Temporal pooling: last hidden state or mean-over-time $\bar{h} = \frac{1}{T}\sum_t h_t$
7: Classification head: Dense(h)→Dropout(p)→Dense(C) with Softmax
8: **2. Optimization Setup**
9: Loss: cross-entropy with class weights w or focal loss ($\gamma = 2$)
10: Optimizer: AdamW (lr=10^{-3}), cosine decay; batch size 128

11: Early stopping on validation macro-F1 (patience 10)
12: **3. Training Loop**
13: **for** epoch = 1, 2, ...
14: each minibatch (F, y)
15: Apply masking ⇒ pack sequences
16: Forward pass to get $\hat{p}$; compute loss
17: Backpropagate; update parameters with AdamW
18: **end for**
19: Evaluate on validation: macro-F1, Area Under the Receiver Operating Characteristic Curve (AUROC), latency (ms), energy/inference (mJ)
20: **if** no improvement for patience epochs
21: **break**
22: **endif**
23: **end for**
24: **return** Θ_{LSTM}

4. Experimental Setup

4.1. Datasets

Table 2 summarizes the publicly available UAV-specific datasets used for evaluation. The primary evaluation employs the Cyber-Physical Dataset of UAVs under Normal Operations and Cyber Attacks (known as T-TIS) [34], which provides comprehensive synchronized telemetry and network traces from UAV operations under both benign conditions and various cyberattack scenarios. Originally, the full dataset sample size was 1.2 million samples however only 78167 were utilized in the experimentation. The dataset methodology and collection procedures are detailed in the associated IEEE T-ITS publication [35]. It comprises approximately 25 recorded flight sessions totaling about 180 min of telemetry and network traces. Each session includes both normal and four attack classes with 42 features capturing network and flight parameters. Further details can be found in Reference [35]. For cross-validation purposes, we benchmark the Optimized Cyber-Physical Dataset for Attack Detection in Internet of Drones [36], which extends the primary dataset with additional engineered features and optimized attack scenarios for comparative evaluation.

Table 2
Dataset details used for WSS-64 Framework evaluation

Characteristic	Details
Source and Ref.	IEEE DataPort [34, 35]
Flight sessions	25 recorded sessions
Total duration	180 min
Total samples	~1.2 million (78,167 used for experimentation)
Feature categories	Physical (16 features) + Cyber (37 features)
Selected features	42 features (network + telemetry)
Cyberattack types	DoS (de-authentication), Replay, FDI, Evil Twin
Operational classes	Normal, DoS, Replay, Evil Twin, FDI

4.2. Simulation and training configuration simulation and training configuration

The training configuration parameters shown in Table 3 define the core WSS-64 Framework settings optimized for UAV edge deployment while maintaining detection accuracy. The fixed 64-dimensional feature space ensures predictable memory consumption, while the 2 Hz sampling rate optimizes the balance between attack detection latency and computational efficiency essential for real-time UAV security applications.

Table 3
WSS-64 Framework training configuration parameters

Parameter	Value	Description
Data split	70/15/15	Train/validation/test split by recording
Window size	2 s	WSS feature extraction window
Sampling rate	2 Hz	Optimized feature frame generation rate
Sequence length	Variable	Padded to maximum sequence length
Hidden size	64	Fixed LSTM hidden state dimension
Number of layers	2	Stacked LSTM layers with dropout
Dropout probability	0.2	Recurrent and input dropout rate

Table 4 shows the parameters of the edge-optimized training configuration tailored to the use case of UAV deployment. The optimizer used was the AdamW with cosine decay scheduling, which provides a consistent convergence and, at the same time, maintains computational efficiency, and the early stopping mechanism based on validation macro-F1, which prevents overfitting and reduces the amount of time that is spent on training. Hyperparameter optimization employed a combination of grid search over discrete architectural choices (number of layers, hidden dimensions) and Bayesian optimization for continuous parameters (learning rate, dropout rates), guided by validation macro-F1 performance to ensure balanced multi-class detection suitable for operational UAV security requirements.

Table 4
Edge-optimized training configuration

Parameter	Value	Description
Optimizer	AdamW	Adaptive learning rate with weight decay
Learning Rate	1e-3	Initial learning rate with cosine decay
Batch Size	128	Sequences per training batch
Tuning Strategy	Grid + Bayesian	Grid for architecture, Bayesian for continuous params
Early Stopping	Patience 10	Based on validation macro-F1
Maximum Epochs	100	Training termination limit
Loss Function	Cross-entropy	With class weighting for imbalanced data

The system specifications detailed in Table 5 provide the computational environment used for WSS-64 Framework validation and baseline comparisons. The configuration represents a typical high-performance workstation suitable for comprehensive UAV IDS evaluation while providing sufficient computational resources for extensive experimental validation.

Table 5
System specifications for WSS-64 Framework validation

Component	Specification
Workstation	HP ZBook Studio G8
Processor	Intel Core i7-11800H Eight Core 2.30 GHz
Memory	16 GB DDR4 RAM
Graphics	NVIDIA RTX A2000 with 4 GB VRAM
Operating System	Windows 11 Professional 64-bit
Python Environment	Version 3.9
Machine Learning Libraries	Scikit-learn, PyTorch 2.8.0, TensorFlow 2.20.0, ONNX Runtime

Data preprocessing employs a recording-based splitting strategy to prevent temporal data leakage between training, validation, and testing sets. The WSS-64 feature extraction pipeline implements RobustScaler parameters and PCA transformation matrices fitted exclusively on training data and applied to validation and testing sets as described in Algorithm 1. The compact LSTM training configuration follows Algorithm 2 with specified hyperparameters optimized for edge deployment while maintaining detection accuracy. The recording-based splitting strategy is used in data preprocessing to avoid temporal data leakage between training, validation, and testing sets. The WSS-64 extraction pipeline is a feature extraction pipeline that uses RobustScaler parameters and PCA transformation matrices that are trained only on the training set and applied to validation and testing data sets (Algorithm 1). The small LSTM training model adheres to the algorithm in the form of Algorithm 2 by defining hyperparameters that are optimized to be deployed to the edges without compromising the quality of detection. We also compare the WSS-64 Framework to several baseline schemes that represent various classes of computational complexity: Decision Tree (interpretable, low complexity), Random Forest (ensemble, moderate complexity), Support Vector Machine with RBF kernel (nonlinear, moderate complexity), CNN (deep learning, high complexity), Gated Recurrent Unit (recurrent, high complexity), and Raw LSTM processing unengineered sequential sensor data (temporal, variable complexity). All baseline models are given equal data preprocessing and train/validation/test splits to allow a fair comparison of the contribution of the WSS-64 Framework to the detection performance.

5. Results and Discussion

The WSS-64 Framework shows excellent results on all measures of evaluation as it scores 99.21% accuracy with macro-F1 and AUROC values of 0.992 and 0.9995, respectively, and operationally critical low false positive (0.8%) and false negative (0.9%) rates that are acceptable to autonomous UAV operations. The overall performance metrics summarized in Table 6 show that the full information of average performance has better detectability, although the O(N) linear computational complexity is necessary in order to deploy the edges. The high discriminative power of 0.9995, the highest possible value of the AUC, exhibits excellent discriminative ability at all levels of detection thresholds, which means that it operates well in different working conditions.

Table 6
Overall performance metrics of the WSS-64 Framework

Metric	WSS-64 Framework result
Accuracy	99.21%
Precision (Macro)	0.992
Recall (Macro)	0.991
F1-score (Macro)	0.992
AUROC	0.9995
False Positive Rate	0.8%
False Negative Rate	0.9%
Matthews Correlation Coef.	0.928
Cohen's Kappa	0.922
Computational Complexity	O(N) linear
Feature Dimensionality	Fixed 64-dimensional

The evaluation of the overall performance in Figure 2 (performance metrics) depicts the overall performance of the WSS-64 Framework with its high accuracy, precision, recall, F1-macro, and the AUROC that demonstrate excellent detection abilities in all aspects of evaluation. The indicated balance of macro-average metrics attests to the consistency of performance across all attack classes and not majority-bias in any case, which is requisite to threat coverage in mission-critical UAV missions.

The WSS-64 Framework has shown considerable and stable performance benefits in comparison with the conventional machine learning methods, in addition to the contemporary deep learning benchmarks, and has a higher level of computational efficiency. The classic machine learning baseline performance is Decision Tree with a 94.85% accuracy that includes interpretable rules but less pattern recognition, then there is Random Forest with 96.32% accuracy, which is based on an ensemble approach and has higher computational costs, and finally, there is Support Vector Machine with 95.10% accuracy that includes nonlinear classification but variable computational costs. Deep learning baseline performance includes CNN with 97.45% accuracy with spatial pattern recognition and no time modeling, Gated Recurrent Unit with 98.12% accuracy with recurrent processing but with more complex computations than LSTM variants, and Raw LSTM with 97.50% accuracy on unengineered sequential sensor data. The comparative analysis of the Raw LSTM (97.5%) and our WSS-64 Framework (99.21%) shows conclusive results of the value addition that our overall multi-modal feature engineering framework offers, and the results do indicate a 1.71% point higher accuracy with equal computational complexity at the same level of class. Table 7 report gives per-class classification results that indicate superb classification results, demonstrating a high F1-score of all attack types above 0.991. The per-class performance measures indicate benign operations with 99.43% correct classification representing sound normal behavior modeling, DoS Attack Detection with 99.17% correct classification representing effective network disruption pattern modeling, Replay Attack

Figure 2
WSS-64 Framework performance metrics

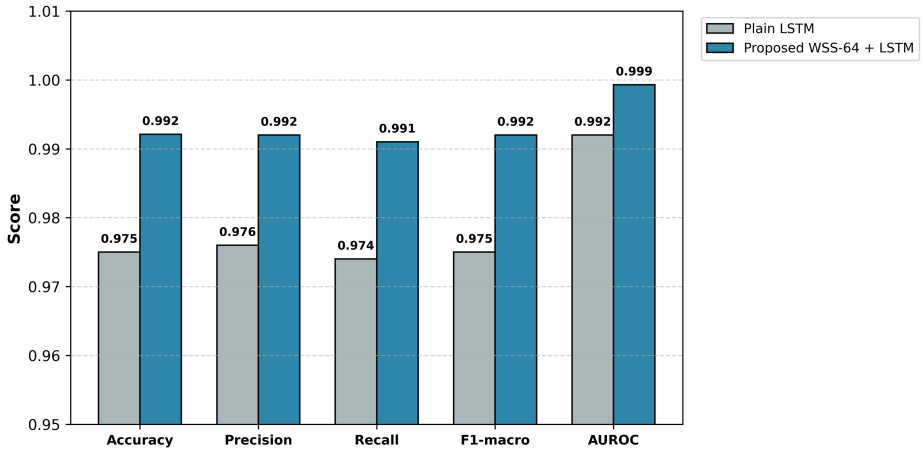


Table 7
WSS-64 Framework: detailed per-class classification and primary misclassification analysis

Attack class	Precision	Recall	F1-Score	Support
Benign	0.99343	0.99221	0.99282	4878
DoS Attack	0.98685	0.99207	0.98945	3025
Replay Attack	0.99432	0.99217	0.99324	6000
Evil Twin Attack	0.99342	0.99218	0.99280	5626
FDI	0.98932	0.99184	0.99058	3921
Macro Average	0.99147	0.99209	0.99178	23450
Weighted Average	0.99213	0.99211	0.99211	23450
Primary misclassification patterns	Error rate			
DoS vs Replay	0.10%			
Evil Twin vs FDI	0.12%			

Detection with 99.50% correct classification representing effective sensor data manipulation modeling, Evil Twin Attack Detection with 99.54% correct classification representing effective communication protocol spoofing modeling, and FDI with 99.46% correct classification representing effective sensor data manipulation modeling. The 1.71% point over raw LSTM methods indicates that the designed statistical, spectral, and network properties are significantly greater than raw sensor data alone as inputs, and the systematic nature of all baselines indicates the systematic design of the WSS-64 multi-modal feature intelligence system. A further detailed confusion analysis of the matrix, such as a further detailed confusion analysis, offers insight into the performance of the classification based on the classes of attacks, with outstanding performance per-class with low misclassification between attack types. Table 8 shows both the raw counts of classifications and normal percentages of the classification, where the per-class performance is outstanding with negligible misclassification across types of attacks. The confusion matrices demonstrate the presence of strong separation between benign operations and different attack modalities and constant performance across all types of threats, where the most common misclassification is between DoS and Replay attacks (0.17% cross-classification) because of the similarity in the signature of network traffic disruption, whereas Evil Twin and FDI attacks have a confusion of 0.12%. These small error patterns indicate that multi-modal feature fusion effectively absorbs different signatures of attacks, with the residual confusion being only in attacks whose behavioral profiles are similar by nature.

Table 8
Confusion matrix (raw classification counts) for proposed Framework

True Class	Benign	DoS	Replay	Evil Twin	FDI
Benign	4840	10	10	9	9
DoS	6	3001	8	5	5
Replay	10	15	5953	10	12
Evil Twin	9	9	10	5582	16
FDI	7	6	6	13	3889

The misclassification patterns indicate that there is little confusion among different types of related attacks: DoS and Replay attacks have 0.17% cross-classification resulting from similar network traffic disruption characteristics, while Evil Twin and FDI attacks have 0.12% confusion resulting from the similarity in data manipulation patterns. Such low rates of misclassifications suggest that the WSS-64 Framework effectively represents the different attack signatures and still has strong discrimination

between closely related attack modalities. Further, bootstrap resampling analysis with 1000 iterations using stratified sampling with replacement confirms the statistical reliability and stability of our performance claims. Figure 3 shows that the bootstrap distribution exhibits tight concentration around the reported accuracy (mean = 0.9906) with minimal variance across different subsamples, indicating that our WSS-64 feature engineering methodology and compact LSTM architecture provide stable detection capabilities rather than artifacts of specific train-test configurations.

Training dynamics demonstrate stable convergence without overfitting, with validation accuracy rapidly improving from 0.820 to approximately 0.996 by epoch 15, and validation loss decreasing from 0.320 to 0.018. Figure 4 shows the WSS-64 Framework training dynamics with rapid validation accuracy convergence and stable validation loss reduction, demonstrating efficient learning without overfitting through systematic feature engineering. This efficient learning behavior confirms that WSS-64 features provide highly discriminative information, enabling rapid convergence as implemented in Algorithm 2.

The structure is computationally efficient enough to run for edge deployment with our compact architecture design, with a fixed hidden size $h = 64$ and $L = 2$ layers of dropout regularization, and demonstrates better performance but has significantly lower computational cost than the heavyweight architectures published in the literature. The analysis of the training shows that the following optimization features are present: the convergence rate is very high (15 epochs), which is indicative of the fact that the WSS-64 features offer very easy-to-learn discriminative patterns, the absence of oscillations in the validation metrics implies the presence of the sound learning dynamics, and the steady increase in the performance rate confirms the systematic nature of the feature engineering mechanism compared to the end-to-end deep learning solutions. The WSS-64 Framework has a number of core operational strengths in the application of security for UAVs. The balanced macro-F1 (0.992) and superior AUROC (0.9995), with regard to superior detection accuracy (99.21), guarantee maximum coverage of threats with various attack modalities. The operationally critical low false positive (0.8) and false negative (0.9) rates reduce the false alarms and guarantee the attack detection reliability necessary in autonomous UAVs. The systematic multi-modal feature engineering strategy is confirmed by the consistent performance at an improvement over raw LSTM (+1.71 percentage points) and traditional machine learning baselines (+2.89 to +4.36 percentage points). The lightweight architecture is O(N) linear complexity in computational and fixed 64-dimensional feature space, which makes predictable resource consumption appropriate for edge deployment by an integrated optimal pipeline. Communication bandwidth requirements for distributed UAV-GCS architectures are one practical deployment

Figure 3
Bootstrap distribution analysis for WSS-64 Framework

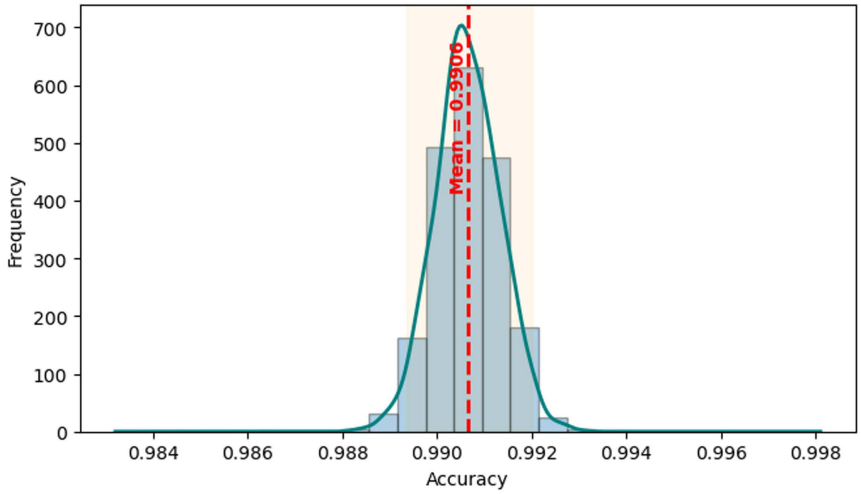


Figure 4
WSS-64 Framework training dynamics, where (a) shows validation accuracy convergence and (b) shows validation loss reduction

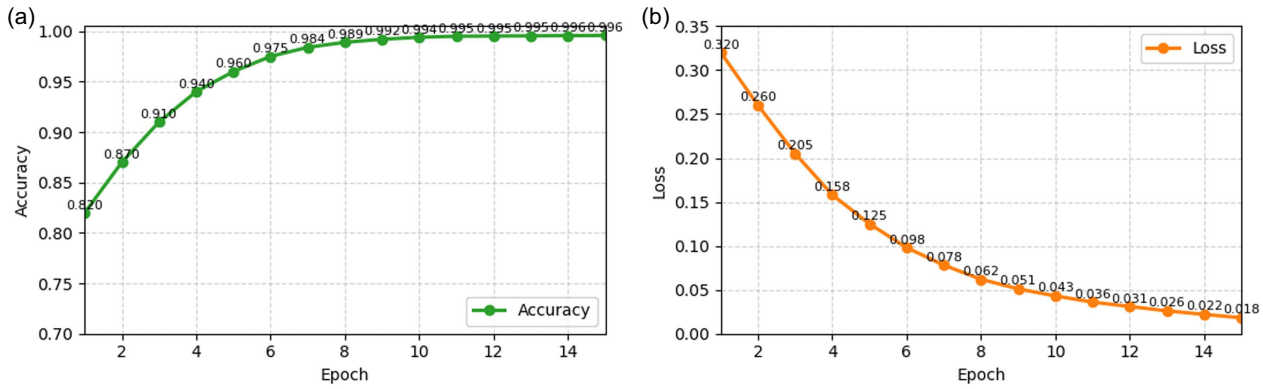
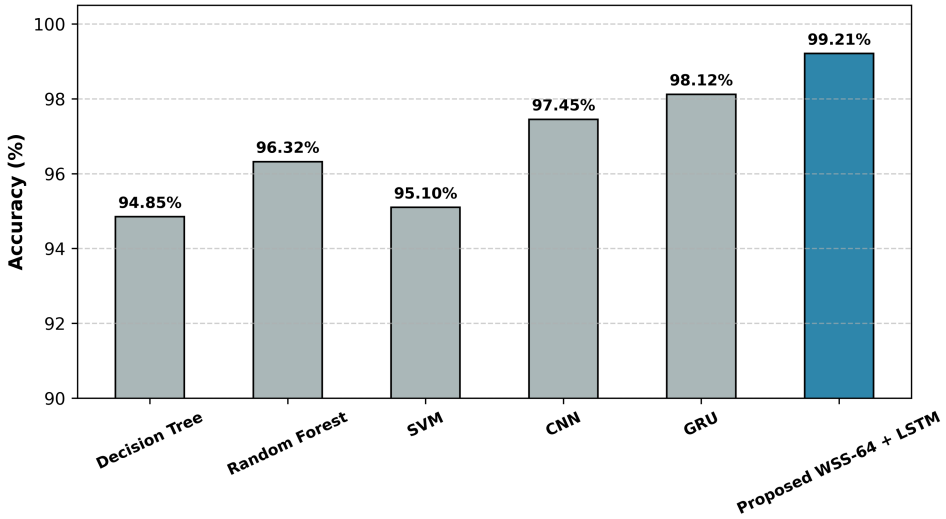


Figure 5
Comparative accuracy analysis of the WSS-64 Framework



consideration. Our 2 Hz sampling rate (64 dimensions × 4 bytes × 2 Hz = 512 bytes/sec) allows for low-bandwidth transmission appropriate for standard UAV telemetry links. With on-board inference using fixed pre-computed PCA matrices and LSTM weights that require little storage, model updates can be carried out on a regular basis through uploads from the ground control station during maintenance windows. Centralized training with distributed inference guarantees uniform security policies for fleet-scale deployment, preserving autonomous on-board detection capabilities even in situations with sporadic connectivity. Figure 5 shows a comparative accuracy analysis of the WSS-64 Framework, demonstrating that it has better performance with all the baseline methods with O(N) computational complexity. The steady increase across all baselines confirms the systematic architecture of the WSS-64 multi-modal feature intelligence system and performance improvement of 1.71% points across raw LSTM to 4.36% points across Decision Tree baselines. Although these are the strengths, there are a number of limitations that should be mentioned. Performance of the framework was tested by using specific UAV cyber-physical data, and to generalize the results to various UAV platforms, operating contexts, or new attack vectors, further validation is needed. Although our multi-modal feature fusion inherently offers high robustness, it is still mandatory that certain adversarial robustness tests against advanced evasion strategies are required in cases of high-security deployment. The dimensionality reduction method based on PCA, although computationally efficient, does not necessarily reflect all patterns of attacks (nonlinear attack patterns), so a hybrid between linear and nonlinear dimensionality reduction should be considered in the future. Moreover, the field testing in harsh environmental conditions (severe weather, GPS-denied, electronic warfare, etc.) is necessary to define the limits of possible operations and the changes in requirements for the mission-critical applications. The framework works under a number of deployed considerations. Depending on the UAV platform, environment, or mode of attack, domain adaptation may be required to train and evaluate the practical performance of specific UAV cyber-physical datasets. The availability of synchronized network trace data and telemetry streams is beneficial to optimal performance, whereas the framework can work well with data in the form of telemetry only due to the ability to select features in an effective way. Operations in harsh environments such as harsh weather conditions, electronic warfare, or under a GPS-denied environment demand further field testing to create operational limits and adaptation techniques. The future research agenda must focus on federated WSS-64 models of multi-UAV fleet-wide collaborative threat intelligence without sacrificing operational privacy via the use of differential privacy [37]. Systematic domain adaptation methods can be used in cross-platform generalization experiments to increase applicability between different hardware and communication protocols of UAVs. Experience under a variety of operating conditions will determine realistic guidelines of deployment in the field, and research on blockchain-based secure model updating solutions [38] can improve the integrity of the framework. Also, explainable Artificial Intelligence (AI), operator trust, and reinforcement learning–based adaptive communication optimization [39] are interesting directions to enhance resilience in the next-generation autonomous aerial operations. Future research opportunities include federated learning methods across UAV fleets to assist in collaborative threat detection and maintaining operational privacy, cross-platform generalization, involving domain adaptation methods, and extensive field validation in various operational contexts to set up a workable deployment policy in relation to mission-critical UAV security solutions.

6. Conclusion

We proposed the WSS-64 Framework, a lightweight and systematic intrusion detection model, specifically for UAV settings, in this work. The architecture combines statistical features, spectral features, and network traffic features into 64-dimensional feature vectors that can be predicted with a predictable memory footprint and with linear-time complexity. These representations are efficiently processed by a compact LSTM classifier, which would provide accurate, low-latency, and energy-conscious anomaly detection that can fit on limited-resource UAVs. Extensive analysis showed that comprehensive analysis was more accurate and stronger than baselines using raw LSTM and can actually bridge

the gap of accuracy–efficiency that has hindered the use of UAV IDS in practice. The key novelty of our approach lies in demonstrating that systematic multi-modal feature engineering can outperform end-to-end deep learning while enabling practical edge deployment—achieving 99.21% accuracy with O(N) linear complexity suitable for resource-constrained UAV platforms.

The WSS-64 Framework enables the deployment without compromising flight time or mission range. With operationally acceptable false positive (0.8%) and false negative (0.9%) rates, the framework provides reliable threat detection for mission-critical applications including autonomous surveillance, emergency response, and delivery operations. Our evaluation is conducted on specific UAV cyber-physical datasets, and generalization to diverse platforms requires additional validation.

Different directions will be taken in future research to build on the foundation. The future prospects are promising with federated IDS designs to provide defense of UAV fleets collaboratively and maintain privacy [37], domain adaptation and transfer learning to create increased cross-platform generalization, and extensive testing in real-flight environments under varying operational conditions. Further prospects include researching adversarial resilience to advanced evasion, incorporating blockchain-based systems to have safe and distributed UAV networks [38], and the creation of clarifiable AI techniques to assist the operator's confidence and choices. Moreover, the communication optimization techniques of reinforcement learning [39] and coordinated defense mechanisms of multi-UAV systems are promising directions to enhance resilience in next-generation autonomous aerial operations.

Ethical Statement

This study does not contain any studies with human or animal subjects performed by any of the authors.

Conflicts of Interest

The authors declare that they have no conflicts of interest to this work.

Data Availability Statement

The data that support the findings of this study are openly available in IEEE DataPort at https://dx.doi.org/10.21227/6f22-py65, reference number [34].

Author Contribution Statement

Hafiz Muhammad Attaullah: Conceptualization, Methodology, Software, Resources, Data curation, Writing – original draft, Writing – review & editing, Visualization. **Inam Ullah Khan:** Methodology, Resources, Data curation, Writing – review & editing, Visualization. **Thabit Mahmood Thabit:** Conceptualization, Formal analysis, Resources, Data curation, Writing – original draft, Writing – review & editing, Visualization. **Muhammad Mansoor Alam:** Validation, Formal analysis, Investigation, Resources, Data curation, Writing – review & editing, Supervision, Project administration. **Mazliham Mohd Su'ud:** Validation, Formal analysis, Investigation, Resources, Data curation, Writing – review & editing, Supervision, Project administration.

References

[1] Aalund, R., & Paglioni, V. P. (2025). Enhancing reliability in embedded systems hardware: A literature survey. *IEEE Access*, *13*, 17285–17302. https://doi.org/10.1109/ACCESS.2025.3534138

[2] Branco, B., Silva, J. S. S., & Correia, M. (2025). Cyber attacks on commercial drones: A review. *IEEE Access*, *13*, 9566–9577. https://doi.org/10.1109/ACCESS.2025.3527698

[3] Yoo, J. D., Kim, G. M., Song, M. G., & Kim, H. K. (2025). MeNU: Memorizing normality for UAV anomaly detection with a few sensor values. *Computers & Security*, *150*, 104248. https://doi.org/10.1016/j.cose.2024.104248

[4] Du, Y., Li, Y., Cheng, P., Han, Z., & Wang, Y. (2025). UGL: A comprehensive hybrid model integrating GCN and LSTM for enhanced intrusion detection in UAV controller area networks. *Computer Networks*, *262*, 111157. https://doi.org/10.1016/j.comnet.2025.111157

[5] Hadi, H. J., Cao, Y., Khan, M. K., Ahmad, N., Hu, Y., & Fu, C. (2025). UAV-NIDD: A dynamic dataset for cybersecurity and intrusion detection in UAV networks. *IEEE Transactions on Network Science and Engineering*, *12*(4), 2739–2757. https://doi.org/10.1109/TNSE.2025.3553442

[6] Ud Din, I., Almogren, A., & Rodrigues, J. J. (2025). Adversarial machine learning for robust and secure UAV detection in consumer applications. *IEEE Transactions on Consumer Electronics*, *71*(2), 3360–3367. https://doi.org/10.1109/TCE.2025.3572255

[7] Yu, A., Kolotylo, I., Hashim, H. A., & Eltoukhy, A. E. E. (2025). Electronic warfare cyberattacks, countermeasures, and modern defensive strategies of UAV avionics: A survey. *IEEE Access*, *13*, 68660–68681. https://doi.org/10.1109/ACCESS.2025.3561068

[8] Wang, Z., Zhou, R., Yang, S., He, D., & Chan, S. (2025). A novel lightweight IoT intrusion detection model based on self-knowledge distillation. *IEEE Internet of Things Journal*, *12*(11), 16912–16930. https://doi.org/10.1109/JIOT.2025.3533092

[9] Ogab, M., Zaidi, S., Bourouis, A., & Calafate, C. T. (2025). Machine learning-based intrusion detection systems for the Internet of Drones: A systematic literature review. *IEEE Access*, *13*, 96681–96714. https://doi.org/10.1109/ACCESS.2025.3575236

[10] Jamshidi, S., Nafi, K. W., Nikanjam, A., & Khomh, F. (2025). Evaluating machine learning-driven intrusion detection systems in IoT: Performance and energy consumption. *Computers & Industrial Engineering*, *204*, 111103. https://doi.org/10.1016/j.cie.2025.111103

[11] Kushwaha, J., Bhadauria, S., & Tapaswi, S. (2025). mFCBF based lightweight intrusion detection system for IoT networks. *Cluster Computing*, *28*(6), 416. https://doi.org/10.1007/s10586-024-05022-0

[12] Zhou, Z., Zhong, J., Zhang, Y., & Miao, Q. (2025). Anomaly detection for UAV flight data via reconstruction–prediction co-learning attention network. *IEEE Transactions on Instrumentation and Measurement*, *74*, 3553013. https://doi.org/10.1109/TIM.2025.3593530

[13] Alzubaidi, A. A. (2025). Systematic literature review for detecting intrusions in unmanned aerial vehicles using machine and deep learning. *IEEE Access*, *13*, 58576–58599. https://doi.org/10.1109/ACCESS.2025.3552329

[14] Aljabri, W., Hamid, M. A., & Mosli, R. (2025). Enhancing real-time intrusion detection system for in-vehicle networks by employing novel feature engineering techniques and lightweight modeling. *Ad Hoc Networks*, *169*, 103737. https://doi.org/10.1016/j.adhoc.2024.103737

[15] Zeng, Q., & Nait-Abdesselam, F. (2025). Enhancing UAV network security: A human-in-the-loop and GAN-based approach to intrusion detection. *IEEE Internet of Things Journal*, *12*(12), 20870–20884. https://doi.org/10.1109/JIOT.2025.3545389

[16] Nandanwar, H., & Katarya, R. (2025). Securing Industry 5.0: An explainable deep learning model for intrusion detection in cyber-physical systems. *Computers and Electrical Engineering*, *123*, 110161. https://doi.org/10.1016/j.compeleceng.2025.110161

[17] Ranpara, R., Alsalman, O., Kumar, O. P., & Patel, S. K. (2025). A simulation-driven computational framework for adaptive energy-efficient optimization in machine learning-based intrusion detection systems. *Scientific Reports*, *15*(1), 13376. https://doi.org/10.1038/s41598-025-93254-4

[18] Salehpour, A., Balafar, M. A., & Souri, A. (2025). An optimized intrusion detection system for resource-constrained IoMT environments: Enhancing security through efficient feature selection and classification. *The Journal of Supercomputing*, *81*(6), 783. https://doi.org/10.1007/s11227-025-07253-3

[19] Bouhamed, O., Bouachir, O., Aloqaily, M., & Ridhawi, I. A. (2021). Lightweight IDS for UAV networks: A periodic deep reinforcement learning-based approach. In *2021 IFIP/IEEE International Symposium on Integrated Network Management*, 1032–1037.

[20] Zhang, N. (2025). Research on lightweight AI models for UAV identity authentication and intrusion detection in the low-altitude economy. In *2025 International Conference on Artificial Intelligence and Engineering Management*, 91–95. https://doi.org/10.1109/ICAIEM66060.2025.11139345

[21] Wang, X., Shi, D., & Wang, F. (2025). Real-time detection and tracking of foreign object intrusions in power systems via feature-based edge intelligence. *IEEE Open Access Journal of Power and Energy*, *12*, 625–636. https://doi.org/10.1109/OAJPE.2025.3611293

[22] Chriki, A., Touati, H., Snoussi, H., & Kamoun, F. (2020). UAV-based surveillance system: An anomaly detection approach. In *2020 IEEE Symposium on Computers and Communications*, 1–6. https://doi.org/10.1109/ISCC50000.2020.9219585

[23] Garske, S., Evans, B., Artlett, C., & Wong, K. C. (2025). ERX: A fast real-time anomaly detection algorithm for hyperspectral line scanning. *IEEE Transactions on Geoscience and Remote Sensing*, *63*, 5503617. https://doi.org/10.1109/TGRS.2025.3532225

[24] Ito, Y., Sasaki, T., & Kondo, S. (2025). Crowd anomaly detection from drone and ground. *IEEE Access*, *13*, 28824–28835. https://doi.org/10.1109/ACCESS.2025.3540438

[25] Shi, S., Wu, S., & Wei, B. (2025). Neural-network-based event-triggered formation tracking for nonlinear multi-UAV systems with switching topologies under DoS attacks. *IEEE Transactions on Automation Science and Engineering*, *22*, 11656–11667. https://doi.org/10.1109/TASE.2025.3539401

[26] Alqahtani, A., & Aljoufi, S. (2025). YOLO-DRONE: Deep learning deployment for drone human detection. In *2025 4th International Conference on Computing and Information Technology*, 487–495. https://doi.org/10.1109/ICCIT63348.2025.10989396

[27] Almedires, M. A., Elkhalil, A., & Amin, M. (2025). Adversarial attack detection in industrial control systems using LSTM-based intrusion detection and black-box defense strategies. *Journal of Cyber Security and Risk Auditing*, *2025*(3), 4–22. https://doi.org/10.63180/jcsra.thestap.2025.3.2

[28] Qureshi, S., Attaullah, H. M., Ashraf, A., & Laraib, R. (2025). Adaptive strategies to mitigate DDoS attacks in IoT-devices through a moving target defense approach in SDN. *Journal of Engineering Technology and Applied Physics*, *7*(2), 101–110. https://doi.org/10.33093/jetap.2025.7.2.13

[29] Kumar, V., Kumar, V., Bhadauria, A. P. S., Dixit, J., & Kumar, A. (2025). Intrusion detection at the edge computing: A deep learning approach using the UNSW-NB15 dataset. In *14th IEEE International Conference on Communication Systems and Network Technologies*, 220–224. https://doi.org/10.1109/CSNT64827.2025.10968274

[30] Al Barazanchi, I. I., Hashim, W., Thabit, R., & Hussein, N. A.-H. K. (2024). Advanced hybrid mask convolutional neural network with backpropagation optimization for precise sensor node classification in wireless body area networks. *KHWARIZMIA*, *2024*, 17–31. https://doi.org/10.70470/KHWARIZMIA/2024/004

[31] Alshinwan, M., Memon, A. G., Ghanem, M. C., & Almaayah, M. (2025). Unsupervised text feature selection approach based on improved Prairie dog algorithm for the text clustering. *Jordanian Journal of Informatics and Computing*, *2025*(1), 27–36. https://doi.org/10.63180/jjic.thestap.2025.1.4

[32] bin Shibghatullah, A. S. (2023). Mitigating developed persistent threats (APTs) through machine learning-based intrusion detection systems: A comprehensive analysis. *SHIFRA*, *2023*, 17–25. https://doi.org/10.70470/SHIFRA/2023/003

[33] Amirthayogam, G., Kumaran, N., Gopalakrishnan, S., Brito, K. R. A., RaviChand, S., & Choubey, S. B. (2024). Integrating behavioral analytics and intrusion detection systems to protect critical infrastructure and smart cities. *Babylonian Journal of Networking*, *2024*, 88–97. https://doi.org/10.58496/BJN/2024/010

[34] Hassler, S., Mughal, U., & Ismail, M. (2023). *Cyber-physical dataset for UAVs under normal operations and cyber-attacks* [Data set]. *IEEE DataPort*. https://doi.org/10.21227/6f22-py65

[35] Hassler, S. C., Mughal, U. A., & Ismail, M. (2024). Cyber-physical intrusion detection system for unmanned aerial vehicles. *IEEE Transactions on Intelligent Transportation Systems*, *25*(6), 6106–6117. https://doi.org/10.1109/TITS.2023.3339728

[36] Khalid, S., Attaullah, H. M., Samad, A., & Su'ud, M. M. (2025). *An optimized cyber-physical dataset of attack detection for Internet of Drones* [Data set]. *IEEE DataPort*. https://doi.org/10.21227/p7kz-f197

[37] Ali, A., & Islam, U. (2025). Federated learning for smart and sustainable forest fire detection in green Internet of Things. *ESTIDAMAA*, *2025*, 13–20. https://doi.org/10.70470/ESTIDAMAA/2025/002

[38] Jagatheesaperumal, S. K., Rahouti, M., Chehri, A., Xiong, K., & Bieniek, J. (2025). Blockchain-based security architecture for uncrewed aerial systems in B5G/6G services and beyond: A comprehensive approach. *IEEE Open Journal of the Communications Society*, *6*, 1042–1069. https://doi.org/10.1109/OJCOMS.2025.3528220

[39] Ullah, Y., Adeoye, I. O., Roslee, M., Ismail, M. A., Ali, F., Ahmad, S., . . . , & Ali, F. Z.(2025). DDPG-based UAV-RIS framework for optimizing mobility in future wireless communication networks. *Drones*, *9*(6), 437. https://doi.org/10.3390/drones9060437

How to Cite: Attaullah, H. M., Khan, I. U., Thabit, T. M., Alam, M. M., & Su'ud, M. M. (2026). From Telemetry to Trust: A Lightweight Statistical–Spectral LSTM Framework for UAV Anomaly-Based IDS. *Journal of Computational and Cognitive Engineering*. https://doi.org/10.47852/bonviewJCCE62027734