International Journal of Automation and Control

ISSN online: 1740-7524 - ISSN print: 1740-7516
https://www.inderscience.com/ijaac

Time series data-driven UAV sensor attack detection: an adaptive graph-time-frequency hybrid approach

Junfeng Chen, Yuhang Zhou, Xingsi Xue

DOI: 10.1504/IJAAC.2028.10078430

Article History:

Received:	22 September 2025
Last revised:	06 November 2025
Accepted:	19 November 2025
Published online:	22 May 2026

Time series data-driven UAV sensor attack detection: an adaptive graph-time-frequency hybrid approach

Junfeng Chen* and Yuhang Zhou

College of Artificial Intelligence and Automation,
Hohai University,
Changzhou, 213200, China
Email: chen-1997@163.com
*Corresponding author

Xingsi Xue

Fujian Provincial Key Laboratory
of Big Data Mining and Applications,
Fujian University of Technology,
Fuzhou, Fujian, 350118, China
Email: jack8375@gmail.com
Email: xue.xingsi@fjut.edu.cn

Abstract: To address the limitations of existing methods in dynamic spatial learning, joint time-frequency analysis, and drift attack detection for UAV sensor security, this paper proposes the graph time-frequency mixed anomaly detection (GTF-MAD) model. Its core innovations include an adaptive clustering mask graph attention network (ACM-GAT) for dynamic sensor correlation learning, a time-frequency dual-stream cross-processing path (TFDSCPP) for deep multi-domain feature fusion, and the TSM-EWMA trend detection method for rapid identification of drift attacks. Experiments on a quadrotor platform confirm GTF-MAD's superior performance, achieving a peak F1-score of 99.71% for bias attacks and reducing drift attack detection latency by 67.2% (from 119 to 39 steps) compared to traditional methods. The model offers a reliable and high-precision solution for real-time UAV sensor security.

Keywords: UAV; unmanned aerial vehicle; sensor attack; anomaly detection; GNN; graph neural network; time-frequency analysis; trend detection.

Reference to this paper should be made as follows: Chen, J., Zhou, Y. and Xue, X. (2026) 'Time series data-driven UAV sensor attack detection: an adaptive graph-time-frequency hybrid approach', *Int. J. Automation and Control*, Vol. 20, No. 7, pp.1–25.

Biographical notes: Junfeng Chen received her PhD from the College of Control Science and Engineering, Zhejiang University, in 2011. She is an Associate Professor at the College of Artificial Intelligence and Automation,

Hohai University, Changzhou, China. From 2016 to 2017, CSC sponsored her as a visiting scholar at the University of Birmingham in the UK. She received the ICSI2016 and CIS2019 Excellent Paper Awards and served as Vice President of Science and Technology for the "Double Innovation Plan" in Jiangsu Province. She has published 100 papers in various journals and is responsible for 30 Research Projects. Her research interests include deep learning, artificial intelligence with uncertainty, and time series forecasting techniques.

Yuhang Zhou received his BE in Electrical Engineering and Intelligent Control from Shandong University of Science and Technology, China, in 2022. He is currently a Master's student of Detection Technology and Automation Device, studying in the College of Artificial Intelligence and Automation, Hohai University, China. His research interests include time series anomaly detection and graph neural network .

Xingsi Xue received his PhD from Xidian University, China, in 2014. He was a post-doc fellow at School of Engineering and Computer Science, Victoria University of Wellington, New Zealand, in 2022 and 2023. Currently, he is a Researcher (Natural Science Research) in the School of Computer Science and Mathematics, Fujian University of Technology. His current research interests include knowledge and data engineering, intelligent computation and machine learning. He has published over 200 research papers in refereed journals and conferences. He is an IEEE Senior Member and an ACM Member.

1 Introduction

Unmanned aerial vehicles (UAVs), owing to their flexibility and efficiency, have found widespread applications in fields such as military reconnaissance, disaster monitoring, and logistics transportation (Wang et al., 2023; Radoglou-Grammatikis et al., 2020). However, with the increasing complexity of UAV missions and the deepening of integration, the security of their sensor data faces severe challenges. Sensors, as core components for UAV environmental perception, can lead to flight control system failure or even crashes if subjected to malicious attacks (e.g., data tampering, signal interference). Now, attacks targeting UAV sensors, such as GPS spoofing and gyroscope bias injection, have become frequent. These attacks not only threaten flight safety but can also be exploited for illicit purposes. Therefore, developing efficient methods for detecting sensor data attacks is crucial for ensuring the security of UAVs.

Traditional anomaly detection methods are mainly categorised into three types: expert systems based on prior knowledge, analytical methods based on physical models, and data-driven methods (Puchalski and Giernacki, 2022). Methods based on prior knowledge are based on manual rules and struggle to cope with complex and variable attack patterns. Physical model-based methods require precise system modelling and exhibit poor adaptability. In contrast, data-driven methods learn features directly from sensor data using machine learning, demonstrating stronger generalisation capabilities. However, current research methods still have the following shortcomings:

- *Insufficient learning of dynamic spatial structures*: Existing methods often employ fixed rules (e.g., K-nearest neighbour, maximal information coefficient) to construct sensor correlation graphs, making it difficult to adapt to dynamically changing sensor relationships during flight.
- *Lack of joint time-frequency-domain analysis*: UAV sensor data is significantly affected by environmental noise and mechanical vibrations, relying solely on time-domain analysis makes it difficult to capture critical frequency domain features.
- *Inadequate fusion of multi-modal information*: The absence of effective fusion mechanisms for time-domain, frequency-domain, and spatial features limits the comprehensiveness of detection.
- *Limited capability in detecting drift attacks*: Traditional static threshold methods exhibit insufficient sensitivity to progressive drift attacks, resulting in high detection latency.

To address the aforementioned issues, we proposes a time-series data-driven attack detection framework for UAV sensor data, known as the graph time-frequency mixed anomaly detection model (GTF-MAD). The main contributions are as follows.

- We have designed an adaptive clustering mask graph attention network (ACM-GAT) that dynamically learns the correlations between sensors and enhances the recognition of abnormal patterns using a masking mechanism.
- We have developed a time-frequency dual-stream cross-processing path (TFDSCPP), which integrates a time-domain multi-scale gated interactive convolution blocks (MGICB) with a frequency-domain adaptive frequency convolutional Mixer (AFCM) to facilitate deep fusion of time-frequency features.
- We propose a trend detection method called TSM-EWMA, which combines Theil-Sen slope estimation, a Markov model, and an exponentially weighted moving average (EWMA) to significantly improve early detection capabilities for drift attacks.

This paper is structured as follows. Section 2 discusses related work. Section 3 outlines the problem modelling and theoretical foundations. In Section 4, we describe the GTF-MAD model. Section 5 presents the simulation experiments and analyses the results. Finally, we conclude in Section 6.

2 Related work

2.1 Classification of security threats to UAVs

Security threats to UAV systems can be categorised into three main types: hardware attacks, wireless network attacks, and sensor attacks. Hardware attacks primarily target the physical components of UAVs. They can disrupt normal operations by damaging or tampering with hardware devices. Wireless Network Attacks exploit vulnerabilities in communication links, allowing malicious activities such as data theft and command forgery.

Sensor attacks specifically target the UAV's perception system and can be classified into three types: bias attacks, drift attacks, and stuck attacks. Bias attacks cause sensor

outputs to deviate from actual values by injecting erroneous data, which can potentially lead to failures in UAV attitude control. Drift attacks create cumulative errors in sensor readings over time, simulating sensor ageing or calibration errors that are difficult to detect with traditional methods. Stuck attacks fix the sensor output at a specific value, leading to stagnation in control system responses. These types of attacks can significantly influence a UAV's navigation, obstacle avoidance, and mission execution capabilities. Sensor attacks, due to their high stealthiness and destructive potential, are a significant focus of current research in UAV security.

Recent studies indicate that sensor attacks account for 37% of security incidents in commercial UAV applications, with drift attacks being particularly challenging to detect due to their gradual nature. It has been observed that sensor attacks can result in cumulative positioning errors, loss of attitude control, or even complete hijacking of the UAV (Nassi et al., 2021). Furthermore, while existing defence mechanisms achieve a 92% detection rate for stuck attacks, the detection rate for drift attacks remains below 65%, revealing a significant research gap (Wei et al., 2024). These attacks not only jeopardise the safety of individual UAVs but can also initiate cascading failures in collaborative swarm operations, underscoring the need for more robust detection mechanisms.

2.2 Evolution of anomaly detection methods

2.2.1 Traditional methods

Early anomaly detection for UAVs primarily relied on traditional methods based on prior knowledge, which can be categorised into three main types: expert systems, physical model-based methods, and threshold detection methods. Expert systems diagnose faults by translating domain expert knowledge into predefined rules. For example, abnormal signals are identified through a manually set rule base in a UAV flight control expert system (Sun and Chen, 2012). However, these systems heavily depend on the completeness of the expert knowledge and struggle to adapt to new attack patterns. Physical model-based methods identify anomalies by creating precise mathematical models. Typical examples include detection strategies based on the extended Kalman filter (EKF) and nonlinear dynamic models (Abbaspour et al., 2017), as well as analytical redundancy estimators constructed using kinematic models (Guo et al., 2018). While these methods provide clear physical interpretability, their performance can degrade due to model mismatches, especially when dealing with complex and variable attack scenarios or when UAVs execute highly manoeuvrable actions. Threshold detection methods, another type of traditional approach, identify anomalies by setting static thresholds.

An example is the unsupervised detection scheme based on encoding and thresholding proposed in previous work (Park et al., 2021). While these methods are simple to implement, fixed thresholds tend to struggle with dynamic changes in flight data and are especially insensitive to progressive drift attacks. Overall, traditional methods often exhibit poor adaptability and limited generalisation capabilities in the face of increasingly complex sensor attacks, leading researchers to explore more flexible, data-driven approaches.

2.2.2 Data-driven methods

With the advancement of deep learning, data-driven anomaly detection methods have shown considerable benefits, evolving through two key stages. In the initial phase, methods primarily relied on long short-term memory (LSTM) network architectures to capture

temporal dependencies for anomaly detection (Ahmad and Zouhair, 2022; Malhotra et al., 2015; Bontemps et al., 2016; Wang et al., 2020, 2019). For instance, a comparative study evaluated various LSTM variants and found that the multi-output convolutional LSTM is well-suited for UAV multidimensional time-series data (Ahmad and Zouhair, 2022). Similarly, the LSTM-RF method was developed to improve temporal feature extraction (Wang et al., 2020). However, while effective for univariate time series, these methods often inadequately accounted for spatial correlations among sensors.

Subsequent research introduced spatio-temporal joint methods, which integrate both spatial and temporal features to significantly improve detection performance. Graph neural networks (GNNs) have become a research hotspot for their ability to explicitly model topological relationships between sensors (Wu et al., 2021). For example, the STADN model uses a graph attention network for spatial dependencies and an LSTM for temporal dependencies (Tian et al., 2023). Masked-SGAT-GRU, developed in recent work, learns dynamic sensor dependencies via a spatial attention mechanism, achieving 93.6% accuracy in gyroscope attack detection (He et al., 2022). The introduction of the Transformer architecture has further enhanced the modelling of long-term temporal dependencies (Vaswani et al., 2017; Wang et al., 2024).

Current trends indicate that GNN methods integrating spatio-temporal features offer significant advantages in detection accuracy and real-time performance. However, reducing computational complexity for on-board deployment remains a key challenge.

2.3 Time-Frequency Analysis Methods

Time-frequency analysis techniques are becoming increasingly important for detecting anomalies in UAV sensors. Their primary strength lies in their ability to capture the dynamic characteristics of signals in both the time and frequency domains simultaneously. The traditional short-time Fourier transform (STFT) serves as a fundamental analysis method, converting non-stationary signals into a joint time-frequency representation using a sliding window technique. An optimisation algorithm proposed in previous research significantly enhanced the time-frequency resolution of the STFT, providing a theoretical foundation for extracting periodic features, such as UAV vibration noise (Durak and Arikan, 2003). However, traditional STFT has limitations, including fixed window sizes and uniform resolution when processing non-stationary flight data.

Time-frequency analysis methods have achieved significant advancements. Wavelet decomposition and stacked denoising autoencoders have been utilised to improve the accuracy of anomaly detection methods (Zhou et al., 2024). The FedFormer model (Zhou et al., 2022) innovatively integrates frequency-domain enhancement with the Transformer architecture. This approach enables the separate modelling of long-term trends and short-term fluctuations through frequency-domain feature decoupling, thereby enhancing the F1 score in attitude sensor anomaly detection by 12.6%. The multi-scale frequency-domain fusion method further tackled noise interference by employing an adaptive frequency band selection mechanism that effectively distinguishes between normal flight vibrations (0.5–5 Hz) and abnormal frequency changes caused by attacks (8–15 Hz) (Dang et al., 2021). Recent research has also shown that combining wavelet packet transforms with depthwise separable convolution can reduce computational complexity by 40% while maintaining a 95% detection accuracy, presenting a viable solution for resource-constrained onboard real-time detection. Table 1 compares various time-frequency analysis methods in terms of resolution and complexity.

Current research challenges are primarily focused on optimising dynamic frequency band selection algorithms and integrating the deep fusion of time-frequency features with spatial topological features. This is especially important during complex UAV manoeuvres, where distinguishing between inherent frequency drift due to attitude changes and abnormal frequency variations caused by attacks has become a critical problem for time-frequency analysis methods to address.

2.4 Trend detection methods

To address the challenge of detecting progressive anomalies in UAV sensor data, trend analysis methods have undergone significant evolution from traditional statistical techniques to machine learning-enhanced approaches. Traditional methods primarily rely on sliding window statistical analysis. In their study, the predictive performance of the simple moving average (SMA) and the EWMA was compared (Johnston et al., 1999). The SMA method establishes a baseline by calculating the mean of data within a specified window. However, it has two main drawbacks: firstly, the fixed window size struggles to adapt to dynamic changes in flight data, and secondly, it exhibits a delayed response to gradually developing drift attacks, resulting in an average detection latency of 119-time steps. On the other hand, while EWMA methods improve sensitivity to recent data by incorporating a decay factor, they remain inadequate in handling nonlinear trends.

The introduction of machine learning techniques has significantly enhanced the effectiveness of trend detection. Both the Mann-Kendall trend test and the innovative trend analysis (ITA) method were utilised to assess parameters related to the refractive index (Agbo et al., 2023). Recent advancements demonstrate that combining deep learning with trend decomposition offers unique benefits: Neural networks can learn complex patterns of environmental noise, thereby enhancing the accuracy of predictions. In contrast, the interpretive framework from traditional trend analysis methods can effectively guide the training of the networks. An example of this integration is an architecture that combines LSTM networks with the Mann-Kendall trend test.

Currently, the main challenges in this research area revolve around balancing detection sensitivity and the rate of false alarms. When UAVs encounter turbulence or perform manoeuvreing actions, the system's inherent nonlinear dynamic characteristics may produce trend features that resemble those of an attack. Additionally, computational efficiency is critical for on-board real-time detection, the average inference time of existing trend analysis methods on embedded processors still requires further optimisation.

3 Problem modelling and theoretical basis

3.1 Graph representation of UAV sensor data

UAV sensor data exhibit characteristics of multivariate time series and their dynamic correlations can be effectively modelled using a graph structure. Let the multivariate data from the UAV sensor network be represented within a given time window $X \in \mathbb{R}^{N \times L}$, where N is the number of sensors and L is the time series length. We model this as a dynamic graph $\mathcal{G}_t = (X_t, A_t)$, where node features $X_t \in \mathbb{R}^{N \times d}$ are the sensor feature vectors at

time t, and the adjacency matrix $A_t \in \mathbb{R}^{N\times N}$ describes the dynamically learned interaction weights. Data is normalised using the Z-score method:

$$x'_{i,t} = \frac{x_{i,t} - \mu_i}{\sigma_i} \tag{1}$$

where μ_i and σ_i are the mean and standard deviation of sensor i, respectively. The sliding window (width K) divides the time-series data into samples $\{\mathbf{X}_{t-K+1}, \mathbf{X}_{t-K+2}, \ldots, \mathbf{X}_t\}$ for prediction and anomaly detection.

This modelling approach combines sensor topology with temporal dynamics, providing a structured input for subsequent graph attention networks and time-frequency analysis.

3.2 Graph attention network (GAT)

A graph attention network (GAT) (Brody et al., 2022) is a type of GNN that utilises an attention mechanism, enabling the adaptive assignment of different weights to nodes in a graph and thereby capturing the dynamic dependencies between nodes. The core idea of GAT is to calculate importance weights between nodes using an attention mechanism and then aggregate information from neighbouring nodes to update the representation of the current node.

The raw attention score e_{ij} between nodes i and j is calculated as:

$$e_{ij} = \text{LeakyReLU}(\vec{a}^T[W\vec{h}_i || W\vec{h}_j]) \tag{2}$$

where $\vec{h}_i$ and $\vec{h}_j$ are the features of node i and node j, respectively. Additionally, W is a feature transformation matrix and $\vec{a}$ is an attention parameter vector. The notation $||$ denotes concatenation. The function LeakyReLU is a variant of ReLU that maintains a slight non-zero slope for inputs less than or equal to 0, thus helping to avoid the 'neuron death' problem commonly associated with standard ReLU activation. The normalised attention weights α_{ij} are obtained via the Softmax function:

$$\alpha_{ij} = \text{softmax}_j(e_{ij}) = \frac{\exp(e_{ij})}{\sum_{k\in\mathcal{N}_i}\exp(e_{ik})} \tag{3}$$

The new node feature representation $\vec{h'}_i$ is a weighted aggregation:

$$\vec{h'}_i = \sigma\left(\sum_{j\in\mathcal{N}_i}\alpha_{ij}W\vec{h}_j\right) \tag{4}$$

where σ is a non-linear activation function. Multi-head attention is used to stabilise the learning process by running K independent attention mechanisms:

$$\vec{h'}_i = \sigma\left(\frac{1}{K}\sum_{k=1}^{K}\sum_{j\in\mathcal{N}_i}\alpha_{ij}^{(k)}W^{(k)}\vec{h}_j\right) \tag{5}$$

GAT achieves the modelling of dynamic relationships between nodes in a graph through its attention mechanism. In the task of UAV sensor data attack detection, GAT can effectively capture spatial dependencies between sensors, providing strong support for subsequent time-frequency analysis and anomaly detection.

3.3 Time-frequency analysis

UAV sensor data, as typical non-stationary time-series signals, exhibit statistical characteristics that change significantly over time. Traditional time-domain analysis methods struggle to effectively capture the local frequency-domain features of signals, while pure frequency-domain analysis cannot reflect how frequency components change over time. Time-frequency analysis (TFA), through a joint time-frequency domain representation, provides a powerful tool for feature extraction from such non-stationary signals.

The short-time Fourier transform (STFT), as a fundamental linear time-frequency analysis method, segments long time-series signals into locally stationary fragments by introducing a sliding window mechanism. Its mathematical expression is:

$$X(m,k) = \sum_{n=0}^{N-1} x[n]\omega[n-m]e^{-j2\pi kn/N} \tag{6}$$

where $x[n]$ is the discrete time-series signal, $\omega[n]$ is a window function of length L (e.g., Hamming window), m is the time index, k is the frequency index, and N is the DFT length.

The Heisenberg Uncertainty Principle constrains the time-frequency resolution of STFT. The choice of window length requires a trade-off between time resolution and frequency resolution. A longer window improves frequency resolution but reduces time resolution, and vice versa.

4 GTF-MAD model design

4.1 Overall framework

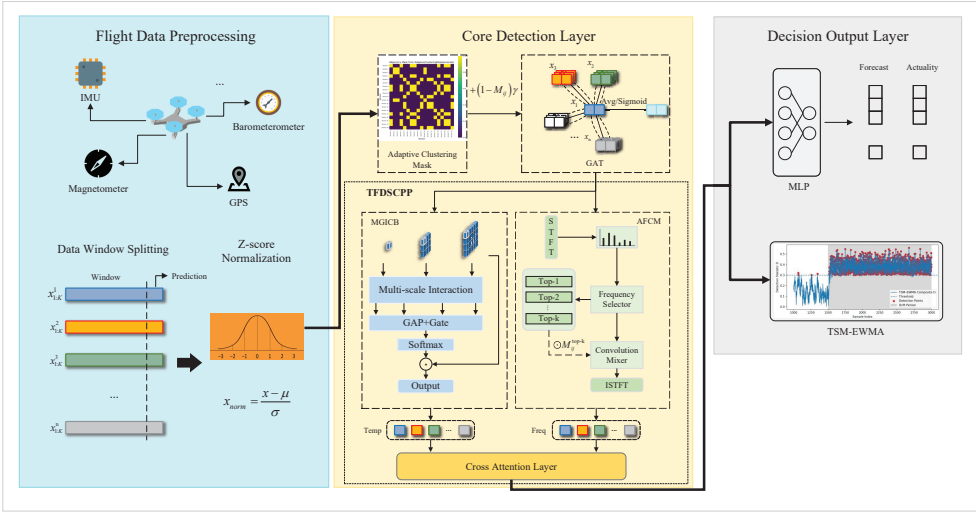
The Graph Temporal-Frequency Mixer Anomaly Detection (GTF-MAD) model is a framework designed for detecting attacks on UAV sensor data using time-series data analysis. Figure 1 illustrates the model's core structure. The model's input consists of multivariate time-series data collected from the UAV. The framework follows a three-stage processing flow: a data preprocessing layer, a core detection layer, and a decision output layer.

The data preprocessing layer standardises multi-source sensor data using sliding-window Z-score normalisation to eliminate scale differences. It extracts fundamental features by converting time-domain signals into time-frequency matrices via the STFT.

The core detection layer utilises a dual-stream architecture for joint spatio-temporal analysis. The spatial stream dynamically models sensor relationships and identifies anomalies using an adaptive clustering masking graph attention network (ACM-GAT). Meanwhile, the temporal stream extracts local temporal features through MGICB in the time domain. It also filters key frequency bands using an AFCM in the frequency domain. Features from both streams are then fused via cross-attention.

Finally, the decision output layer computes anomaly scores using a multi-layer perceptron (MLP), specifically identifying gradual drift attacks through the TSM-EWMA method. It generates real-time anomaly alerts, classifies attack types, and provides a visual analysis interface to support decisions regarding UAV security protection.

Figure 1 GTF-MAD overall architecture (see online version for colours)



4.2 Adaptive clustering mask graph attention network

ACM-GAT is a dynamic GNN specifically designed for anomaly detection in UAV sensor data. Its main innovations include an adaptive clustering mask generator that dynamically learns the inter-sensor correlations through differentiable clustering. This process creates a graph structure that accurately reflects the current flight status. Additionally, ACM-GAT features a mask-enhanced attention mechanism that uses the generated mask to adjust attention weights, allowing it to prioritise strongly correlated sensors while minimising the impact of abnormal nodes.

4.2.1 Adaptive clustering mask generator

ACM-GAT dynamically learns the correlations between sensors to generate an adaptive mask, thereby enhancing anomaly detection capabilities. Input sensor data $X \in \mathbb{R}^{N \times L}$ (where N is the number of sensors and L is the length of the time window) are mapped to low-dimensional features $H_i \in \mathbb{R}^d$ for each sensor's time-series data via an embedding network. A feature attention module calculates the importance weights α_i for each sensor embedding, producing weighted feature embeddings $\tilde{H}_i = \alpha_i \cdot H_i$. The weighted sensor feature embeddings $\tilde{H}_i$ are then used for differentiable clustering. The distance between each sensor embedding and learnable cluster centres C_k is calculated as:

$$d_{i,k} = -\beta_k \|\tilde{H}_i - C_k\|_2^2 \tag{7}$$

where β_k is a learnable affinity parameter for the kth cluster. This distance metric measures the degree of deviation between sensor data and a specific cluster. Simply put, a smaller distance indicates that the sensor's data pattern is closer to the average behavioural pattern represented by that cluster's centre.

The Gumbel-Softmax function processes the negative distances to obtain the soft assignment probability $p_{i,k}$ that sensor i belongs to cluster k. An adaptive adjacency mask

$M_{u,v}$ is constructed based on cluster assignments, reflecting the probability or strength that sensors u and v belong to the same cluster within the current time window:

$$M_{u,v} = \sum_{k=1}^{K} p_{u,k} \cdot p_{v,k} \tag{8}$$

4.2.2 Masked graph attention learning

The mask $M_{u,v}$ is integrated into the graph attention mechanism. The attention scores, modulated by the mask, are normalised via the Softmax function to obtain the final attention coefficients α_{ij}:

$$\alpha_{ij} = \frac{\exp(\text{LeakyReLU}(\vec{a}^T[Wh_i \| Wh_j]) + \lambda M_{i,j})}{\sum_{k \in \mathcal{N}_i} \exp(\text{LeakyReLU}(\vec{a}^T[Wh_i \| Wh_k]) + \lambda M_{i,k})} \tag{9}$$

where λ is a predefined penalty factor. These attention coefficients are then used to perform a weighted aggregation of information from neighbouring sensors, updating the representation of each sensor node:

$$h_i' = \sigma\left(\sum_{j \in \mathcal{N}_i} \alpha_{ij} W h_j\right) \tag{10}$$

The core strengths of ACM-GAT lie in its dynamic adaptability and sensitivity to anomalies. Its real-time masking mechanism captures the changing correlations between sensors during different flight states. When an injection attack occurs, the data pattern from the compromised sensor deviates from its expected trajectory, which alters its relationships with other standard sensors in the clustering space. This change is directly reflected in the mask, allowing the GAT to focus on sensors that demonstrate strong correlations based on the current data pattern or to identify sensor pairs that show broken correlations. As a result, it can more effectively detect subtle anomalies caused by injection attacks. This end-to-end joint optimisation design enables the model to identify sophisticated attack patterns, ensuring robust security for UAVs efficiently.

4.3 Time-frequency dual-stream cross-processing path

TFDSCPP is a core module of the GTF-MAD model designed to enhance the detection of abnormal patterns in UAV sensor data through a joint analysis of time-domain and frequency-domain features. Its design includes several key components: a multi-scale gated interactive convolution block (MGICB) for extracting local temporal features and an AFCM to identify critical frequency bands and reduce noise. The features extracted from both pathways are integrated through a cross-attention mechanism, which uses multi-head attention to facilitate time-frequency interaction. This approach enhances the model's sensitivity and robustness to complex attack patterns, including drift and bias.

4.3.1 Time-domain analysis

To address the dynamic characteristics of UAV sensor time-series data, we have designed a Multi-scale Gated Interactive Convolution architecture, as illustrated in Figure 2. This architecture extracts features using three convolution kernels of varying sizes. After

undergoing non-linear transformation, these features are combined through four interactive fusion methods:

$$B_1 = \text{GeLU}\left(\text{Conv}_{1\times1}\left(h'\right)\right) \odot \text{Conv}_{1\times3}\left(h'\right) \tag{11}$$

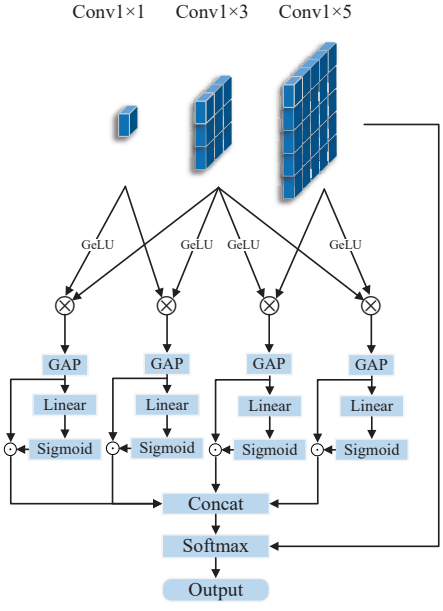
$$B_2 = \text{GeLU}\left(\text{Conv}_{1\times3}\left(h'\right)\right) \odot \text{Conv}_{1\times1}\left(h'\right) \tag{12}$$

$$B_3 = \text{GeLU}\left(\text{Conv}_{1\times3}\left(h'\right)\right) \odot \text{Conv}_{1\times5}\left(h'\right) \tag{13}$$

$$B_4 = \text{GeLU}\left(\text{Conv}_{1\times5}\left(h'\right)\right) \odot \text{Conv}_{1\times3}\left(h'\right) \tag{14}$$

where $\text{Conv}_{1\times k}$ represents 1D convolutions with kernel size k, and $\odot$ denotes element-wise multiplication.

Figure 2 Structure of the multi-scale gated interactive convolution blocks (see online version for colours)



To further adaptively adjust the importance of each interactive path, global average pooling (GAP) is applied to obtain compressed features. The initial weights are generated through a gating mechanism:

$$z_i = \sigma(\text{Linear}(\text{GAP}(B_i))) \odot \text{GAP}(B_i), \quad i = 1, 2, 3, 4 \tag{15}$$

where Linear contains learnable weights and σ is the Sigmoid activation function.

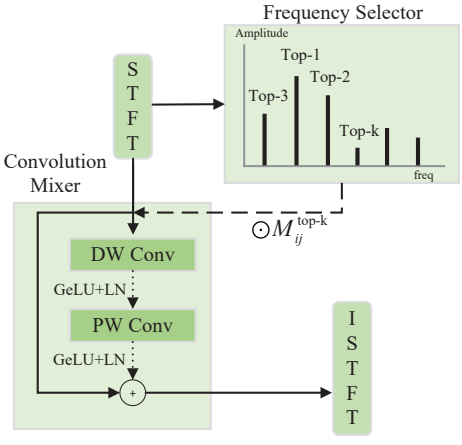
The four weights are concatenated and normalised via Softmax to obtain the final weight vector $\alpha = [\alpha_1, \alpha_2, \alpha_3, \alpha_4]$, which is used to modulate the features of each path. Finally, the paths are weighted, fused, and projected through a 1×1 convolution to obtain the module output:

$$H_t = \text{Conv}_{1\times1}\left(\sum_{i=1}^{4} \alpha \cdot B_i\right) \tag{16}$$

4.3.2 Adaptive frequency-domain analysis

Frequency-domain analysis focuses on extracting essential features from the spectral representation of UAV sensor data to identify anomalies in frequency components that may arise from mechanical vibrations, noise, or attacks. The primary goal is to enhance the model's sensitivity to specific threats, such as drift attacks, through frequency-domain processing while minimising the impact of noise interference. This paper presents an improved AFCM, with the processing flow illustrated in Figure 3.

Figure 3 Structure of the adaptive frequency convolutional mixer (see online version for colours)



As shown in Figure 3, the key steps and innovative designs of AFCM are as follows: STFT preprocessing converts time-domain signals into a time-frequency matrix $h(t, f)$, providing basic spectral features. We denote $h_c(t, f)$ as the time-frequency representation for the cth sensor channel. Adaptive selection is performed for each channel using the amplitude $|h(t, f)|$. The average amplitude of each frequency component for each channel is calculated, and the DC component is zeroed out. The top-k frequency components with the largest average amplitude in each channel are selected to construct a mask function $M_c(f)$ (defined as whether f belongs to the set of top-k indices for channel c), yielding a restricted frequency-domain representation:

$$\tilde{h}_c(t, f) = h_c(t, f) \cdot M_c(f) \tag{17}$$

A depthwise separable convolution structure is used in the following manner. First, a 1D depthwise convolution (DWConv) processes each channel independently along the frequency axis. Next, pointwise convolution (PWConv) is applied to fuse information across channels. This process is complemented by Layer Normalisation (LN) and a non-linear activation function, such as GeLU, to transform the features. The core operation can be expressed as follows:

$$H'_{\text{mid}} = \text{GeLU}(\text{LN}(\text{DWConv}(\tilde{h}_c(t, f)))) \tag{18}$$

$$H'_f = \text{GeLU}(\text{LN}(\text{PWConv}(H'_{\text{mid}}))) + \tilde{h}_c(t, f) \tag{19}$$

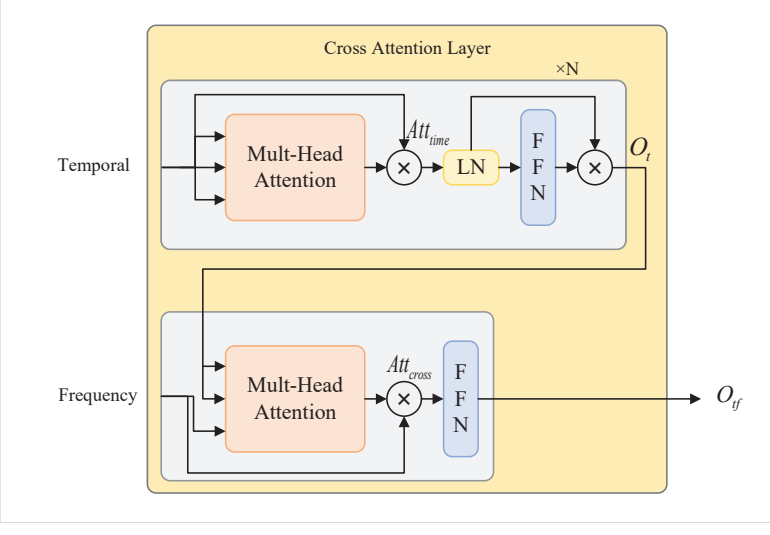
where $\tilde{h}_c(t, f)$ denotes the top-k masked time-frequency matrix calculated as described above, reflecting the time-frequency matrix of the top k frequencies in channel c.

Finally, an inverse fast Fourier transform (IFFT) converts the frequency-domain features back to the time domain H_f for use by subsequent modules.

4.3.3 Time-frequency feature fusion

Time-frequency feature fusion aims to combine the features extracted by the time-domain path (MGICB) and the frequency-domain path (AFCM), achieving deep interaction through a cross-attention mechanism to enhance the model's comprehensive perception of complex abnormal patterns, as detailed in Figure 4.

Figure 4 Structure of the time-frequency cross-attention fusion module (see online version for colours)



Key steps in the time-frequency cross-attention fusion module include multi-head attention (MHA), time-frequency cross-attention, and feature fusion and output. The multi-head self-attention layer formulas are:

$$\text{MHA}\,(Q, K, V) = \text{softmax}\left(\frac{QK^T}{\sqrt{\frac{d}{H}}}\right)V \tag{20}$$

where Q, K, V are query, key, and value respectively, and H is the total number of heads. Att_{time} (time-domain self-attention) and Att_{cross} (time-frequency cross-attention) are computed as follows:

$$Att_{time} = \text{MHA}(Q_{time}, K_{time}, V_{time}) \tag{21}$$

$$Att_{cross} = \text{MHA}(Q_{time}, K_{time}, V_{freq}) \tag{22}$$

The time-frequency cross-attention output is computed through a feed-forward network (FFN):

$$O_{tf} = \text{FFN}(Att_{cross}) \tag{23}$$

$$\text{FFN}(x) = \sigma(xW_1 + b_1)W_2 + b_2 \tag{24}$$

where $W_1, W_2 \in \mathbb{R}^{d\times d}$ and $b_1, b_2 \in \mathbb{R}^d$ represent the weight matrices and bias vectors of the FFN, respectively, and $\sigma(\cdot)$ is a non-linear activation function (e.g., GeLU or ReLU).

4.4 TSM-EWMA

TSM-EWMA significantly enhances the detection efficiency of progressive drift attacks in UAV sensor data through a triple mechanism: robust trend estimation (TSM), dynamic state modelling (MK, referring to the Markov model), and smoothing optimisation (EWMA). Its core lies in achieving early identification of minor trend deviations through robust trend estimation and dynamic smoothing.

Theil-Sen Median trend estimation calculates the slope for all pairs of data points within a window and takes the median of all these slopes as the final trend estimate:

$$\text{slope}_{median} = \text{median}\left(\frac{x_j - x_i}{j - i}\right) \quad \forall i < j \tag{25}$$

The intercept is estimated using $\hat{b} = \text{median}\{x_i - \hat{m}t_i\}$, and a trend function $\hat{x}_t = \hat{m}t + \hat{b}$ is constructed. The residual is then defined as $r_t = x_t - \hat{x}_t$. A discrete set of states $S = \{s_1, s_2, ..., s_k\}$ is introduced, and the residual for the next time step is predicted using a state transition probability matrix P:

$$\hat{r}_{t+1} = P \cdot r_t \tag{26}$$

To further mitigate the impact of noise and short-term fluctuations, the residual sequence is smoothed using EWMA, Specifically, formula (27) demonstrates how to compute the smoothed residual value s_t. This is achieved by assigning a weight α to the current residual r_t and combining it with the historical smoothed average s_{t-1}. This process smooths out random noise in the time series while remaining highly sensitive to the persistent, subtle bias characteristic of drift attacks, thereby significantly enhancing detection speed. The parameter α (smoothing factor) determines the influence of the current residual on the new average value.

$$s_t = \alpha \cdot r_t + (1 - \alpha) \cdot s_{t-1} \tag{27}$$

Finally, an anomaly is considered to exist at a given time if the smoothed residual satisfies:

$$|s_t| > \mu_s + k \cdot \sigma_s \tag{28}$$

where σ_s is the standard deviation of the smoothed residual sequence, and k is a predefined threshold (typically set to 3). This method, while suppressing short-term noise interference, can accurately identify anomalies caused by trend deviations, significantly improving detection accuracy and robustness.

5 Experimental verification and result analysis

5.1 Experimental setup

5.1.1 Experimental environment

To thoroughly assess the performance of the GTF-MAD model, we conducted a series of multidimensional comparative experiments. These included comparisons of prediction performance, evaluations of attack detection capabilities, and analyses of computational efficiency. All experiments were carried out in a consistent experimental environment. The hardware platform featured an NVIDIA RTX 4070 Super GPU, while the software environment included Python 3.9 and PyTorch 2.2.2.

5.1.2 Data and baseline models

To validate the effectiveness of the proposed method, data were collected using a self-developed quadrotor UAV platform. The UAV was equipped with an open-source Pixhawk flight controller and various sensors, including an accelerometer and gyroscope, a barometer, a compass, and a Ublox Neo-M8N GPS module. Twelve types of flight status variables were collected, including angular rate, acceleration, barometric altitude, and GPS position.

Experiments were conducted in an indoor test field, where multiple sets of flight trajectory data were gathered. Samples were generated using a sliding window approach (window width $K = 40$) and were divided into training, validation, and test sets in the ratio of 7:2:1. Baseline models included traditional time-series models (CNN, TCN, and Transformer) as well as anomaly detection models (LSTM-VAE, MTAD-GAT, and Masked-SGAT-GRU). The models were trained using the Adam optimiser with a learning rate of 0.0008 and a batch size of 256. An early stopping condition was implemented, which was triggered when the validation set metrics did not improve for 15 consecutive epochs.

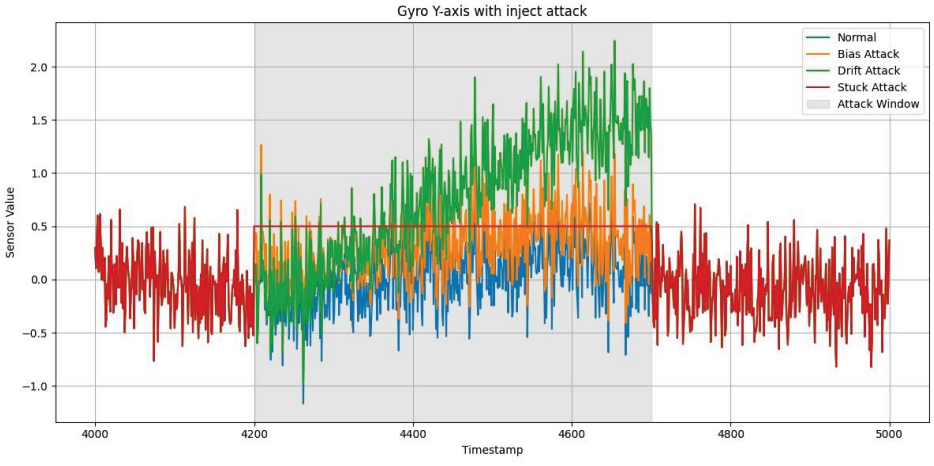
5.1.3 Attack settings

To verify the effectiveness of the detection method, three typical sensor attacks were simulated and injected into normal flight data: bias attack, drift attack, and stuck attack.

- *Bias attack*: A constant offset is added to the sensor data.
- *Drift attack*: A linearly increasing offset over time is introduced.
- *Stuck attack*: Sensor data are fixed to the average value of the 5 timestamps preceding the attack.

The target of the attack was the y-axis of the gyroscope. The test set contained approximately 30,000 timestamps. Examples of attack injections are shown in Figure 5. Anomaly detection was achieved by comparing prediction residuals with a threshold, thereby validating the model's sensitivity to different attacks.

Figure 5 Gyroscope data normal, injected with three types of attacks (bias, drift, and stuck) (see online version for colours)



5.1.4 Evaluation metrics

(1) Prediction performance metrics, including mean squared error (MSE), mean absolute error (MAE) and root mean squared error (RMSE).

$$\text{MSE} = \frac{1}{n}\sum_{i=1}^{n}(Y_i - \hat{Y}_i)^2 \tag{29}$$

$$\text{MAE} = \frac{1}{n}\sum_{i=1}^{n}|Y_i - \hat{Y}_i| \tag{30}$$

$$\text{RMSE} = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(Y_i - \hat{Y}_i)^2} \tag{31}$$

(2) Attack detection metrics:

$$\text{Precision} = \frac{TP}{TP + FP} \tag{32}$$

$$\text{Recall} = \frac{TP}{TP + FN} \tag{33}$$

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \tag{34}$$

$$F1 = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \tag{35}$$

$$\text{FPR} = \frac{FP}{FP + TN} \tag{36}$$

TP (True Positive), FP (False Positive), TN (True Negative), and FN (False Negative).

5.2 Comparative experiments

5.2.1 Prediction performance comparison

Table 2 shows the performance of various models in the multivariate time-series prediction task. Although prediction performance is not the direct goal of anomaly detection, good prediction ability can provide a more accurate baseline for subsequent anomaly detection.

Table 1 Performance of various time-frequency analysis methods for detecting UAV sensor attacks

Method category	*Frequency resolution*	*Time resolution*	*Computational complexity*
STFT	Medium	Medium	Low
Wavelet Transform	Variable	High	Medium
FedFormer	Medium	Medium	High
Deep Freq. Domain Net.	Adaptive	Adaptive	Medium

Table 2 Prediction performance metrics of different models

Model	$MSE(10^{-2})$	$MAE(10^{-2})$	$RMSE(10^{-2})$	*Params* (M)
CNN	0.81487	6.51447	8.98263	0.010
TCN	1.03484	7.23647	10.03685	0.104
Transformer	0.90999	6.79451	9.40844	0.112
LSTM-VAE	0.87161	6.68061	9.21291	0.480
MTAD-GAT	0.84777	6.59854	9.09352	0.241
Masked-SGAT-GRU	0.90025	7.32640	9.4875	0.271
GTF-MAD	0.85000	6.71521	9.16309	0.112

The results in Table 2 quantify model performance on the Time Series Forecasting task using RMSE and MAE. The CNN model, which excels at extracting local temporal features, achieves the best prediction metrics. However, it is essential to distinguish this from our primary goal: Anomaly Detection. A strong forecaster is not necessarily a strong detector. Effective anomaly detection for UAV sensor attacks relies less on minimising short-term prediction error, and more on accurately modelling the dynamic global spatial correlations among heterogeneous sensors. The fixed, local receptive field of CNN limits its ability to capture these critical inter-sensor structural patterns. Conversely, our proposed GTF-MAD model, by integrating GNN components, is specifically designed to prioritise learning these non-local structural behaviours. This structural awareness, which is paramount for attack identification, is why GTF-MAD achieves superior performance in the core detection metrics (F1-score, Precision) shown in Table 2, despite a marginal trade-off in the general forecasting metrics of Table 3.

5.2.2 Attack detection performance comparison

For three typical attack scenarios (bias, drift, stuck), we compared the core detection metrics of each model, as shown in Tables 3–5.

Table 3 Bias attack detection results

Model	*F1*	*Precision*	*Accuracy*	*FPR*	*AUC*
CNN	0.8763	0.9933	0.8652	0.0081	0.82
TCN	0.9857	0.9719	0.9824	0.0446	0.84
LSTM-VAE	0.8744	0.9899	0.8636	0.0124	0.81
MTAD-GAT	0.8755	0.9927	0.8650	0.0089	0.86
Masked-SGAT-GRU	0.8830	0.7905	0.8393	0.4083	0.86
GTF-MAD	*0.9971*	*0.9943*	*0.9965*	*0.0089*	*0.87*

Table 4 Drift attack detection results

Model	*F1*	*Precision*	*Accuracy*	*FPR*	*AUC*
CNN	0.9300	0.8691	0.9361	0.1110	0.83
TCN	0.9470	0.8993	0.9525	0.0825	0.85
LSTM-VAE	0.9461	0.8978	0.9517	0.0839	0.84
MTAD-GAT	0.9540	0.9121	0.9591	0.0710	0.86
Masked-SGAT-GRU	0.9573	0.9181	0.9622	0.0657	0.86
GTF-MAD	*0.9595*	*0.9222*	*0.9642*	*0.0622*	*0.87*

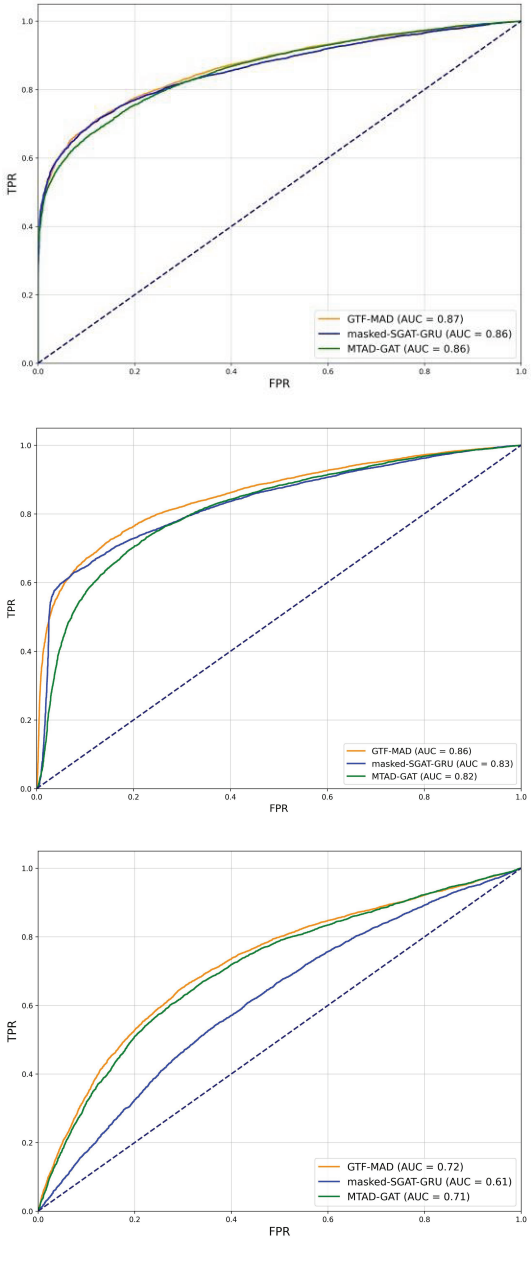
Table 5 Stuck attack detection results

Model	*F1*	*Precision*	*Accuracy*	*FPR*	*AUC*
CNN	0.9551	0.9141	0.9585	0.0744	0.81
TCN	0.9421	0.8905	0.9457	0.0973	0.80
LSTM-VAE	0.9705	0.9427	0.9732	0.0481	0.83
MTAD-GAT	0.9833	0.9671	0.9850	0.0269	0.85
Masked-SGAT-GRU	0.9714	0.9443	0.9740	0.0466	0.84
GTF-MAD	*0.9938*	*0.9877*	*0.9945*	*0.0099*	*0.88*

The GTF-MAD model demonstrates excellent overall performance across various attack detection scenarios. In bias attack detection, the model achieved an F1-score of 0.9971, an improvement of 1.14% points over the next best model, TCN, showcasing its precise identification capability for sudden attacks. For the more stealthy drift attacks, GTF-MAD achieved the lowest false positive rate (FPR) of 0.0622, reflecting its superior stability in anomaly discrimination. Particularly noteworthy is its performance in the stuck attack detection task, where the model, with a precision of 0.9877, significantly surpassed other comparative methods, validating its sensitive detection capability for solidified abnormal data patterns. These results fully demonstrate the comprehensiveness and reliability of the GTF-MAD model in UAV sensor security protection, enabling it to counter different types of malicious attack threats effectively.

Figure 6 illustrates the ROC curve performance of the GTF-MAD model under three different attack scenarios. The ROC curves collectively indicate that GTF-MAD performs robustly across all three attack types, with a pronounced advantage in bias and drift attacks, reflecting the effectiveness of its modular design (e.g., dynamic graph attention, time-frequency fusion). Although stuck attacks are more challenging to detect, the model still maintains relative competitiveness.

Figure 6 ROC curves for different attack scenarios: (a) bias attack (AUC = 0.87 for GTF-MAD); (b) drift attack(AUC = 0.86 for GTF-MAD) and (c) stuck attack(AUC=0.72 for GTF-MAD) (see online version for colours)



5.3 Computational efficiency analysis

In terms of computational efficiency, as shown in Table 6, GTF-MAD demonstrates a well-rounded advantage by achieving superior resource utilisation while maintaining high-

performance anomaly detection capability. Compared to other graph-based neural network approaches, the model exhibits improved computational efficiency over Masked-SGAT-GRU, and particularly outperforms MTAD-GAT with 46.4% decrease in inference latency and a 49.5% reduction in memory usage, significantly lowering computational resource demands. Energy consumption measurements show that GTF-MAD maintains per-sample energy usage below 0.203 mJ, a low-power characteristic that makes it especially suitable for deployment on resource-constrained onboard UAV platforms. These strengths enable GTF-MAD to meet the stringent requirements of UAV systems for real-time performance and lightweight deployment, while ensuring detection accuracy, thereby providing a reliable technical solution for practical engineering applications.

5.4 Ablation experiment

Comparative model variants include the complete GTF-MAD (baseline model), No ACM-GAT (adaptive clustering mask graph attention network removed), No MGICB (Multi-scale Gated Interactive Convolution Block removed), No AFCM (AFCM removed), and No CA (Cross-Attention fusion module removed). Evaluation metrics are Precision, Accuracy (ACC), and FPR. Attack scenarios cover bias attacks (sudden), drift attacks (progressive), and stuck-at attacks (static anomaly).

Table 6 Performance metrics of various models during the inference phase (averaged over the test set)

Model	*Latency* (ms/sample)	*Memory* (MB)	*Energy consumption* (mJ/sample)
Transformer	0.01018	0.13477	0.75573
LSTM-VAE	0.01881	0.13477	0.85748
MTAD-GAT	0.02544	0.26660	0.74135
Masked-SGAT-GRU	0.01451	0.13477	0.57425
GTF-MAD	0.01364	0.13477	0.20264

The results of the ablation study, shown in Table 7, confirm that each component of GTF-MAD is crucial to its overall performance. Removing any module degraded detection capability, but certain components proved essential for specific threats. The ACM-GAT module was most critical, its removal caused a substantial 14% drop in precision for bias attacks and a sharp rise in the FPR for both bias and stuck attacks, highlighting the importance of dynamic graph learning. The time-frequency stream was also vital, as removing the time-domain MGICB module hurt drift attack detection, while removing the frequency-domain AFCM module compromised robustness against bias attacks. The cross-attention (CA) module was shown to be effective for feature fusion and generalisation across all scenarios. These findings validate our synergistic, modular design.

5.5 Specific detection of drift anomalies

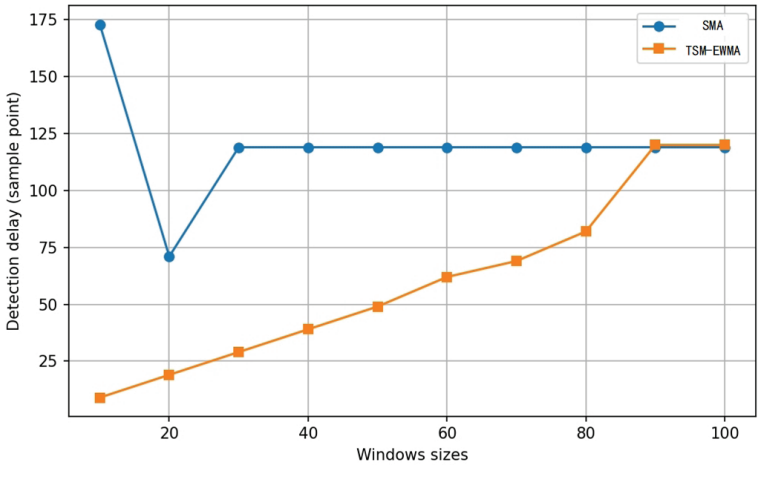
We conducted a comprehensive evaluation of the performance of the proposed TSM-EWMA method against three traditional methods (SMA, EWMA, and LSTM-based residual detection) in detecting drift anomalies. The experiments utilised UAV gyroscope x-axis sensor data, with three test scenarios set up at different drift rates: low-speed drift ($0.002t$, where t is the time step), medium-speed drift ($0.008t$), and high-speed drift ($0.015t$).

In each scenario, the drift attack was injected starting from the 4000th time point. To comprehensively assess detection performance, we introduced four key metrics: Detection Delay, FPR, Early Detection Gain, and Stability Score (the standard deviation of detection delay).

Table 7 Ablation experiment results

Attack type	*Model variant*	*Precision* (↑)	*ACC* (↑)	*FPR* (↓)
Bias attack	GTF-MAD	0.98636	0.99294	0.01441
	No ACM-GAT	0.84754(–14%)	0.90818	0.18756
	No MGICB	0.97802(–0.8%)	0.98853	0.02343
	No AFCM	0.89465(–9.3%)	0.93989	0.12277
	No CA	0.93252(–5.5%)	0.96306	0.07546
Drift attack	GTF-MAD	0.94590	0.97574	0.04214
	No ACM-GAT	0.93302(–1.4%)	0.96955	0.05289
	No MGICB	0.89966(–4.9%)	0.95268	0.08218
	No AFCM	0.92105(–2.6%)	0.96364	0.06315
	No CA	0.91569(–3.2%)	0.96094	0.06784
Stuck attack	GTF-MAD	0.99009	0.99558	0.00791
	No ACM-GAT	0.84420(–14.7%)	0.91850	0.14595
	No MGICB	0.84736(–14.4%)	0.92045	0.14246
	No AFCM	0.84485(–14.7%)	0.91890	0.14523
	No CA	0.85622(–13.5%)	0.92584	0.13281

Figure 7 Comparison of detection delays for various sliding window sizes (see online version for colours)



We systematically evaluated four different drift anomaly detection methods. The traditional SMA method uses a fixed window size of $W = 40$. The EWMA method uses a smoothing factor $\alpha = 0.2$. The LSTM-based residual method constructed a single-layer LSTM network with 64 hidden units and a prediction window of 10 time-steps. The TSM-EWMA method proposed in this paper uses a Theil-Sen median estimator with a window size of 40, combined with EWMA filtering (smoothing factor $\alpha = 0.1$). This is obtained from Figure 7.

Tables 8 and 9 show that the TSM-EWMA method exhibits significant advantages across all key metrics for drift anomaly detection. In terms of detection delay, this method maintained the lowest values in all test scenarios. Specifically, in the medium-speed drift (0.008t) scenario, its detection delay was only 39 time steps, which is 80 time steps shorter than the traditional SMA method (119 time steps), achieving a 67.2% improvement in detection efficiency. This significant performance advantage is primarily attributed to the robust capability of the Theil-Sen estimator within the method to capture trend changes and the early recognition mechanism of the Markov model for abnormal states. In terms of stability, TSM-EWMA's stability score was the best among all compared methods, with scores of 12.7, 10.2, and 8.5 in the three test scenarios, respectively. These are significantly lower than other methods, indicating that this approach can maintain stable detection performance across different drift scenarios. This triple mechanism works synergistically, enabling TSM-EWMA to identify minor trend deviations earlier and more reliably than traditional methods, providing a valuable response time window for UAV systems.

Table 8 Comparison of detection performance at various drift rates

Method	*Drift rate*	*Detection delay*	*Early detection gain*	*Stability score*
SMA	0.002t	187	–	23.4
	0.008t	119	–	18.7
	0.015t	62	–	15.2
EWMA	0.002t	153	18.2%	19.8
	0.008t	98	17.6%	16.3
	0.015t	51	17.7%	13.5
LSTM Residual	0.002t	132	29.4%	25.6
	0.008t	85	28.6%	21.4
	0.015t	45	27.4%	17.8
TSM-EWMA	0.002t	93	50.3%	12.7
	0.008t	39	67.2%	10.2
	0.015t	22	64.5%	8.5

Table 9 Performance comparison of various methods for drift attack detection

Method	*Brief core principle*	*Detection delay (time steps)*	*Window size*
SMA	Residual threshold detection based on simple moving average	119	40
TSM-EWMA	Method combining trend estimation and exponentially weighted smoothing	39	40

6 Conclusion

This paper addresses the critical issue of malicious attacks on UAV sensor data by introducing the GTF-MAD framework. Our model significantly enhances the identification of abnormal patterns by dynamically learning inter-sensor correlations through an ACM-GAT and improves robustness by integrating time-domain and frequency-domain features

via a TFDSCPP. Notably, our innovative TSM-EWMA trend detection method reduces the detection latency for drift attacks from 119 to just 39 time steps, outperforming existing methods in various attack scenarios.

Future research will focus on developing lightweight real-time detection techniques suitable for resource-constrained UAV platforms, enhancing the model's generalisation to unknown attack types, and improving the system's interpretability for better integration with autonomous control systems. This work provides an effective solution for UAV sensor security and lays the groundwork for next-generation intelligent UAV protection systems.

Acknowledgements

This work is supported by the National Key Research and Development Program of China (2022YFB4703404).

Conflicts of interest

All authors declare that they have no conflicts of interest.

References

Abbaspour, A., Aboutalebi, P., Yen, K.K. and Sargolzaei, A. (2017) 'Neural adaptive observer-based sensor and actuator fault detection in nonlinear systems: Application in UAV', *ISA Transactions*, Vol. 67, pp.317–329, DOI: 10.1016/j.isatra.2017.01.023.

Agbo, E.P., Nkajoe, U. and Edet, C.O. (2023) 'Comparison of Mann-Kendall and Şen's innovative trend method for climatic parameters over Nigeria's climatic zones', *Climate Dynamics*, Vol. 60, No. 11, pp.3385–3401, DOI: 10.1007/s00382-022-06485-6.

Ahmad, A. and Zouhair, D. (2022) 'Using MLSTM and multioutput convolutional LSTM algorithms for detecting anomalous patterns in streamed data of unmanned aerial vehicles', *IEEE Aerospace and Electronic Systems Magazine*, Vol. 37, No. 7, pp.6–15, DOI: 10.1109/MAES.2022.3160534.

Bontemps, L., Cao, V.L., McDermott, J. and Le-Khac, N.A. (2016) 'Collective anomaly detection based on long short-term memory recurrent neural networks', *International Conference on Future Data and Security Engineering*, Springer, Cham, pp.141–152, DOI: 10.1007/978-3-319-47650-8_11.

Brody, S., Alon, U. and Yahav, E. (2022) 'How attentive are graph attention networks?', *Proceedings of the 10th International Conference on Learning Representations (ICLR)*, Virtual Conference.

Dang, H.V., Tran-Ngoc, H., Nguyen, T.V., Bui-Tien, T., De Roeck, G. and Nguyen, H.X. (2021) 'Data-driven structural health monitoring using feature fusion and hybrid deep learning', *IEEE Transactions on Automation Science and Engineering*, Vol. 18, No. 4, pp.2087–2103, DOI: 10.1109/TASE.2020.3025219.

Ding, C., Sun, S. and Zhao, J. (2023) 'MST-GAT: A multimodal spatialtemporal graph attention network for time series anomaly detection', *Information Fusion*, Vol. 89, pp.527–536, DOI: 10.1016/j.inffus.2022.08.030.

Durak, L. and Arikan, O. (2003) 'Short-time fourier transform: Two fundamental properties and an optimal implementation', *IEEE Transactions on Signal Processing*, Vol. 51, No. 5, pp.1231–1242, DOI: 10.1109/TSP.2003.810313.

Guo, D., Zhong, M. and Zhou, D. (2018) 'Multisensor data-fusion-based approach to airspeed measurement fault detection for unmanned aerial vehicles', *IEEE Transactions on Instrumentation and Measurement*, Vol. 67, No. 2, pp.317–327, DOI: 10.1109/TIM.2017.2764124.

He, K., Yu, D., Wang, D., Chai, M., Lei, S. and Zhou, C. (2022) 'graph attention network-based fault detection for UAVs with multivariant time series flight data', *IEEE Transactions on Instrumentation and Measurement*, Vol. 71, pp.1–13, DOI: 10.1109/TIM. 2022.3185311.

Johnston, F.R., Boyland, J.E., Meadows, M. and Shale, E. (1999) 'Some properties of a simple moving average when applied to forecasting a time series', *Journal of the Operational Research Society*, Vol. 50, No. 12, pp.1267–1271, DOI: 10.1057/palgrave.jors.2600833.

Malhotra, P., Vig, L., Shroff, G. and Agarwal, P. (2015) 'Long short term memory networks for anomaly detection in time series', *Proceedings of the 23rd European Symposium on Artificial Neural Networks, Computational Intelligence and Machine Learning (ESANN)*, Bruges, Belgium, pp.89–94.

Nassi, B., Bitton, R., Masuoka, R., Shabtai, A. and Elovici, Y. (2021) 'SoK: Security and privacy in the age of commercial drones', *2021 IEEE Symposium on Security and Privacy (SP)*, IEEE, San Francisco, CA, USA, pp.1434–1451, DOI: 10.1109/SP40001.2021.00082.

Park, K.H., Park, E. and Kim, H.K. (2021) 'Unsupervised Fault Detection on Unmanned Aerial Vehicles: Encoding and Thresholding Approach', *Sensors*, Vol. 21, No. 6, p.2208, DOI: 10.3390/s21062208.

Puchalski, R. and Giernacki, W. (2022) 'UAV fault detection methods, state-of-the-art', *Drones*, Vol. 6, No. 11, p.343, DOI: 10.3390/drones6110343.

Radoglou-Grammatikis, P., Sarigiannidis, P., Lagkas, T. and Moscholios, I. (2020) 'A compilation of UAV applications for precision agriculture', *Computer Networks*, Vol. 172, Art. No. 107148, DOI: 10.1016/j.comnet.2020.107148.

Sun, X.C. and Chen, X.P. (2012) 'Design of UAV flight control system fault diagnosis expert system', *Equipment Manufacturing Technology*, University of Wollongong, Wollongong, NSW, Australia, pp.66–68.

Tian, Z., Zhuo, M., Liu, L., Chen, J. and Zhou, S. (2023) 'Anomaly detection using spatial and temporal information in multivariate time series', *Scientific Reports*, Vol. 13, No. 1, p.4400, DOI: 10.1038/s41598-023-31518-7.

Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A.N., Kaiser, L. and Polosukhin, I. (2017) 'Attention Is All You Need', *Advances in Neural Information Processing Systems 30 (NIPS)*, pp.5998–6008.

Wang, B., Wang, Z., Liu, L., Liu, D. and Peng, X. (2019) 'Data-Driven Anomaly Detection for UAV Sensor Data Based on Deep Learning Prediction Model', *Prognostics and System Health Management Conference (PHM-Paris)*, IEEE, Paris, France, pp.286–290, DOI: 10.1109/PHM-Paris.2019.00057.

Wang, B., Liu, D., Peng, Y. and Peng, X. (2020) 'Multivariate regressionbased fault detection and recovery of UAV flight data', *IEEE Transactions on Instrumentation and Measurement*, Vol. 69, No. 6, pp.3527–3537, DOI: 10.1109/TIM.2019.2949313.

Wang, Z., Zhu, H., Sun, Z., and Liu, P. (2023) 'A survey on cybersecurity attacks and defenses for unmanned aerial systems', *Journal of Systems Architecture*, Vol. 138, Art. No. 102870, DOI: 10.1016/j.sysarc.2023.102870.

Wang, S., Liu, Z., Jia, Z., Tang, Y., Zhi, G. and Wang, X. (2024) 'Fault detection for UAVs with spatial-temporal learning on multivariate flight data', *IEEE Transactions on Instrumentation and Measurement*, Vol. 73, pp.1–17, DOI: 10.1109/TIM.2023.3340636.

Wei, X., Ma, J. and Sun, C. (2024) 'A survey on security of unmanned aerial vehicle systems: Attacks and countermeasures', *IEEE Internet of Things Journal*, Vol. 11, No. 21, pp.34826–34847, DOI: 10.1109/JIOT.2023.3274246.

Wu, Z., Pan, S., Chen, F., Long, G., Zhang, C. and Yu, P.S. (2021) 'A Comprehensive Survey on Graph Neural Networks', *IEEE Transactions on Neural Networks and Learning Systems*, Vol. 32, No. 1, pp.4–24, DOI: 10.1109/TNNLS.2020.2978386.

Zhou, T., Ma, Z., Wen, Q., Wang, X., Sun, L. and Jin, R. (2022) 'Fedformer: Frequency enhanced decomposed transformer for long-term series forecasting', *Proceedings of the 39th International Conference on Machine Learning (ICML)*, Baltimore, MD, USA, pp.27268–27286.

Zhou, S., He, Z., Chen, X. and Chang, W. (2024) 'An Anomaly Detection Method for UAV Based on Wavelet Decomposition and Stacked Denoising Autoencoder', *Aerospace*, Vol. 11, No. 5, p.393, DOI: 10.3390/aerospace11050393.