10.48047/jocaaa.2020.28.06.15

Context Aware Transformer with Graph Attention Intrusion Detection Systemfor UAV Enabled Fog Computing Networks

Dipti Prava Sahu[1] Dr. B. L. Raina[2]

[1]Research Scholar, Computer Science & Engineering, Glocal University, Uttar Pradesh
[2]Professor, Computer Science & Engineering, Glocal University, Uttar Pradesh

Corresponding author email: diptiprava29@gmail.com

Abstract

The integration of unmanned aerial vehicles (UAVs) with fog computing has rapidly expanded in applications such as military surveillance, disaster response, smart agriculture, traffic monitoring, and healthcare delivery. Recent studies report that nearly 70% of UAV communication systems are exposed to cyber vulnerabilities, while denial-of-service and replay attacks contribute to a major portion of UAV network disruptions in fog-assisted environments. However, conventional manual monitoring systems and traditional signature-based intrusion detection approaches often experience delayed attack identification, poor scalability, high computational complexity, and limited adaptability to dynamic cyber threats. To address these challenges, this study proposes an intelligent UAV based Fog Computing driven Cyber Intrusion Detection System (UAV-FC-CIDS) using the UAV-NIDD dataset for attack detection and classification. Initially, preprocessing techniques such as noise removal, missing value handling, normalization, and data balancing are applied to improve dataset quality and learning efficiency. Then, a Context Aware Parametric Numerical (CAPN) Transformer is utilized for extracting deep contextual and numerical traffic features from UAV communication data. Finally, a Graph Attention Convolution Network (GACN) classifier accurately categorizes network traffic into Benign, Denial of Service (DoS) attacks, and Replay attacks by learning adaptive graph-based communication relationships within the fog computing environment. Finally, the proposed UAV-FC-CIDS achieved 99.91% of accuracy, 99.88% of precision, 99.84% of recall, and 99.86% of F1-score, which are superior than traditional systems.

Keywords: Classification, Cybersecurity, Fog Computing, Intrusion Detection, Transformer, Unmanned Aerial Vehicles

1. Introduction

The development of UAVs embedded into fog computing environments has revolutionized the intelligent communication system in current era, especially in the areas of defense, disaster monitoring, smart transportation, precision agriculture and emergency healthcare applications [1]. Newly published investigations of the UAV communication infrastructure have revealed that over 70% of the communication infrastructure is vulnerable to cyber-attacks, because of using wireless communication channels that are not secure and the distributed nature of fog interaction [2]. In addition, denial of service attacks and replay attacks are cited as accounting for almost 45% of incidents in an autonomous UAV-assisted network, which can cause disruption to communication, leakage of data, delay in mission completion, and instability in operations [3]. The proliferation of UAVs in critical real-time applications has thus driven greater importance of having a secure, scalable and intelligent IDS to defend distributed aerial communication systems from evolving threats in cyber space.

But existing manual intrusion monitoring methods and conventional rule-based cyber security systems have a few practical drawbacks in highly dynamic environments of UAV-fog communications. Current security systems rely on a pre-defined set of attack signatures and manual intervention to monitor intrusion activity and patterns, which are inefficient in terms of detecting patterns that are new or changing very quickly [4]. Additionally, manual traffic inspection also brings delayed response time, high computation load, high false alarm rate, and poor scalability in processing huge amount of UAV communication streams. Conventional machine learning methods also fail to successfully model temporal communication dependency, contextual interaction, and structure relationships among distributed UAV nodes, which leads to lower accuracy of intrusion detection in real-world fog computing environment.

10.48047/jocaaa.2020.28.06.15

To address such restrictions, sophisticated Artificial Intelligence (AI) algorithms have come to the fore as a very promising approach to intelligent UAV cybersecurity management. An AI-powered IDS [5] can learn the patterns of communication, adapt to changing attack techniques and offer real-time threat detection without a lot of human oversight [6]. In fog networks, deep learning and graph-based protocols are especially well suited for the efficient extraction of contextual traffic information, the modeling of communication dependency for adapting communications, and the intelligent classification of attacks in distributed fog networks. The combination of transformer-based contextual learning [7] with graph attention convolution will substantially boost the accuracy of IDSs, decrease false-positive alerts, increase scalability, and offer comprehensive protection against advanced UAV cyberattacks, like DoS and Replay [8]. So, the novel contributions of this work as follows:

- To develop a novel UAV-FC-CIDS framework that integrates CAPN Transformer learning with GACN classification for intelligent UAV cyber intrusion detection in fog computing environments.
- To introduce a context-adaptive numerical attention mechanismcapable of capturing temporal communication behavior, node interaction patterns, and attack-sensitive UAV traffic characteristics from distributed fog-assisted aerial networks.
- To design an adaptive graph attention-driven intrusion classification model that accurately identifies Benign, DoS, and Replay attacks with improved detection accuracy.

In the rest of this paper, Section 2 is a general survey of the current trends in the field of UAV cyber intrusion detection and fog computing security systems. The proposed methodology is described in detail in Section 3; experimental results and performance analysis are discussed in Section 4, and the paper is concluded in Section 5 with key findings and future research directions.

2. Literature Survey

In [9], authors introduced a lightweight federated generative AI system called GenFed-IDS for anomaly detection on unmanned aerial vehicles (UAVs). The methodology combined federated learning with the generative AI anomaly modeling approach to facilitate distributed intrusion detection while maintaining data privacy among UAV nodes. In [10], authors surveyed the comprehensive field of intrusion detection in AI-enabled smart urban ecosystems, focusing on machine learning, deep learning, and federated security mechanisms. In [11], authors introduced the framework of Spatio-Temporal Graph Neural Network (ST-GNN) for zero-day intrusions detection in low altitude autonomous UAV swarms. The approach adopted was based on graph neural learning with temporal dependency modeling to uncover hidden attack propagation patterns among connected UAV nodes.

In the context of UAV swarms, in [12] authors introduced a Byzantine-Robust Federated Learning (BRFL) system for cross-modal intrusion detection that leverages Vision Transformers (ViT). In this methodology, visual feature extraction using transformer models was combined with federated learning to enhance secure communication and attack resilience in distributed UAV systems. In [13], authors proposed a lightweight intrusion detection framework for UAV and FANET environment, which is based on Federated Graph Neural Networks (FGNN), Deep Temporal Convolution Network (DTCN), and Long Short-Term Memory (LSTM) models. In [14], authors proposed an adversarial robust UAV-IDS, which is designed using AdvGAN and decision boundary reconstruction techniques. The methodology has produced samples used in the adversarial phase and reconstructed classification boundaries to enhance the robustness to adversarial perturbation attacks.

In the work of [15], an all-in-one Lightweight Temporal-Spatial (LTS)- Transformer model is proposed for detection of intrusions in drone communication networks. The approach utilized temporal sequence learning and spatial dependency extraction to detect malicious communication behaviors in UAV traffic streams. In [16], authors proposed a zero-shot attack detection mechanism for the UAV network security based on foundation models. In secure communication systems [17], authors introduced secure communication protocols in combination with intelligent-based anomaly detection systems for UAV and ground communication systems. The methodology was centered on secure protocol management and AI-based behavior monitoring to ensure secure UAV communication.

To detect intrusion by unmanned aircraft in short-range applications, in [18] authors presented a sector-scanning ultrasonic radar-emulation system. The approach used was based on ultrasonic sensing and radar emulation techniques to identify intrusions by unauthorized UAVs in a local monitoring context. To address UAV intrusion

10.48047/jocaaa.2020.28.06.15

detection [19], authors suggested a comparative machine learning study with the technique of cyber-physical data fusion. In [20], authors developed an intrusion detection framework named RoboLSTM-IDS using deep learning techniques that was tested on various datasets of UAV networks. The methodology used to implement LSTM based temporal learning to detect sequential attack actions and enhance classification accuracy of intrusion in UAV communication system.

3. Proposed Methodology

The framework of UAV-FC-CIDS, as depicted in Figure 1, proposes a novel hybrid cyber-IDS for UAV assisted fog computing systems, which combines with the advanced contextual learning and graph-based attack classification mechanisms that have never been studied together within the context of UAVs, fog computing system and CIDS. The UAV-NIDD dataset is then passed through an adaptive preprocessing pipeline that involves noise removal, redundant traffic filtering, missing value reconstruction, min-max normalization, and attack-balance for imbalanced data to improve the quality of the UAV communication data. Then a novel designed CAPN Transformer is used as the feature extraction module, which integrates parametric numerical embedding and contextual dependency learning to extract the temporal communication behavioural features, node interaction patterns, and the attack-sensitive traffic features from the distributed UAV-fog transmissions. Unlike the conventional transformer models, the proposed CAPN framework dynamically highlights the numerical communication relationship in a context-dependent manner using context-adaptive attention mapping, which enhances the discriminative feature representation of intrusion-related traffic analysis. Subsequently, the multi-dimensional contextual features extracted are fed into a GACN classifier, which dynamically constructs graph relationships among the UAV communication nodes, and applies adaptive attention-driven convolution learning to detect unknown propagation patterns of cyberattacks in fog-enabled aerial networks. The combination of contextual parametric transformer learning and graph attention convolution modeling yields a novel hybrid model that can learn both temporal and structural attack behavior and relational structure. Further, the proposed framework provides an accurate classification of network traffic and improves the detection accuracy of both DoS attacks and Replay attacks, while minimizing false alarm rate, increasing the scalability, and ensuring robust real-time cybersecurity protection for UAV fog computing applications with intelligence.

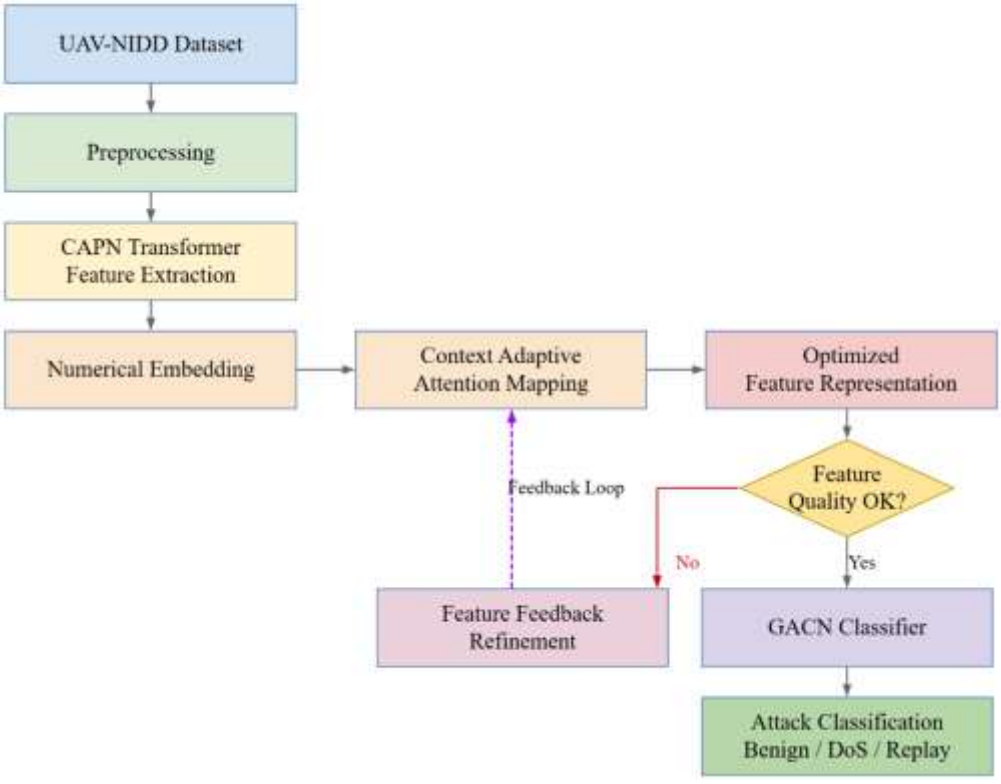

Figure 1. Proposed UAV-FC-CIDS System Architecture.

10.48047/jocaaa.2020.28.06.15

3.1 CAPN Transformer Feature Extraction

The CAPN-Transformer illustrated in Figure 2 aims to gather communication features with high discriminative power and high context-awareness from UAV network traffic in a fog computing environment. The main goal of the CAPN framework is to identify hidden numerical relationships, temporal communication patterns, protocol interactions and attack-related contextual relationships in UAV data streams. The proposed CAPN model is different from the existing transformer models, as it does not only emphasize the traffic characteristics related to intrusion by sequential attention learning, but also introduces parametric numerical adaptation to focus on security-relevant traffic characteristics dynamically. First, the UAV communication data is preprocessed and converted into numerical embedding representations, and then the subsequent steps involve contextual attention learning, adaptive parametric weighting, feature correlation optimization, and nonlinear dependency enhancement. The CAPN framework can successfully distinguish benign communication behaviors from malicious communication behaviors like DoS and Replay attacks by passing through the multiple stages of contextual transformation. Finally, the optimized contextual representations are combined into a compact feature vector of high dimensionality and sent to the GACN classifier for intrusion categorization. The preprocessed UAV traffic data is a numerical input matrix for the contextual learning:

$$X = \{x_1, x_2, x_3, \dots, x_n\} \tag{1}$$

In this case, X represents the full set of UAV communication data (with n traffic instances). The i^{th} network communication sample is represented as x_i, which includes protocol, packet, temporal and routing attributes. This formulation is the first structured representation of contextual feature extraction. The numerical embedding layer maps the raw UAV communication values to a dense parametric representation:

$$E_i = W_e x_i + b_e \tag{2}$$

The UAV traffic sample is embedded in a vector E_i, wherethis is the embedding vector. The trainable embedding weight matrix is denoted as W_e denotes the embedding bias vector as b_e. This step maps heterogeneous communication attributes to a common numerical feature space. The temporal communication dependencies are preserved by having the positional contextual encoding:

$$PE(pos, 2j) = \sin\left(\frac{pos}{10000^{2j/d}}\right) \tag{3}$$

In this case, PE refers to positional encoding, pos to sequence position, and $j$indices$x$ of embedding dimension. Further, $d$corresponds to feature dimensionality. This sinusoidal encoding preserves the sequential encoding behavior of the UAVs through time periods. The cosine positional encoding component is:

$$PE(pos, 2j+1) = \cos\left(\frac{pos}{10000^{2j/d}}\right) \tag{4}$$

Cosine encoding is used here to complement sinusoidal encoding for alternate positional dimensions. The overall coding scheme is designed to enhance learning of contextual dependency for UAV packet transmission sequences. It increases the ability to detect temporal changes during feature extraction in intrusive mode. The contextual attention mechanism calculates the relevance of the communication between UAV traffic instances:

$$A(Q, K, V) = \text{Softmax}\left(\frac{QK^T}{\sqrt{d_k}}\right)V \tag{5}$$

In this case, the matrices are called query, key, and value matrices, and are denoted by the letters Q, K, and V. Here, d_k represents key dimensionality for normalisation. This is an attention operation that detects crucial communications interactions related to malicious intrusion behaviour. The query matrix generation is given by:

$$Q = EW_Q \tag{6}$$

Here, Q is the contextual query matrix extracted from embedding representations E. The trainable query transformation matrix is denoted as $W_Q$denotes. This operation is used to learn communication request patterns in UAV traffic flows. The key matrix transformation is defined to be:

$$K = EW_K \tag{7}$$

10.48047/jocaaa.2020.28.06.15

Here, K denotes the contextual key matrix that captures feature matching relationships. Further, W_K represents trainable key transformation weights. This process helps to discover the correlated attack communication characteristics. The value matrix learning operation is represented by:

$$V = EW_V \tag{8}$$

In this formulation, the representation of contextual value for attention aggregation is vindicated. Here, W_V denotes a value transformation matrix, which were learned. This operation maintains the meaningful information about the UAV communication during contextual learning. A parametric contextual weighting operation increases the emphasis of attack-sensitive features:

$$P_i = \alpha_i \cdot A_i + \beta_i \tag{9}$$

Here, P_i denotes the optimized parametric contextual feature vector of the i^{th} traffic sample. The adaptive scaling parameters α_i and bias parameters β_i are represented. This mechanism dynamically enhances attributes related to the communication needed for intrusion. Finally, we combine the extracted contextual features as optimized deep feature vectors:

$$F = \sum_{i=1}^{n} P_i \tag{10}$$

Here, F represents the output of the final contextual feature sent to the GACN classifier. Further, P_i is used to denote individual optimized parametric representations of features. The aggregation process results in compact and highly discriminative features for UAV communication with intrusion.

10.48047/jocaaa.2020.28.06.15

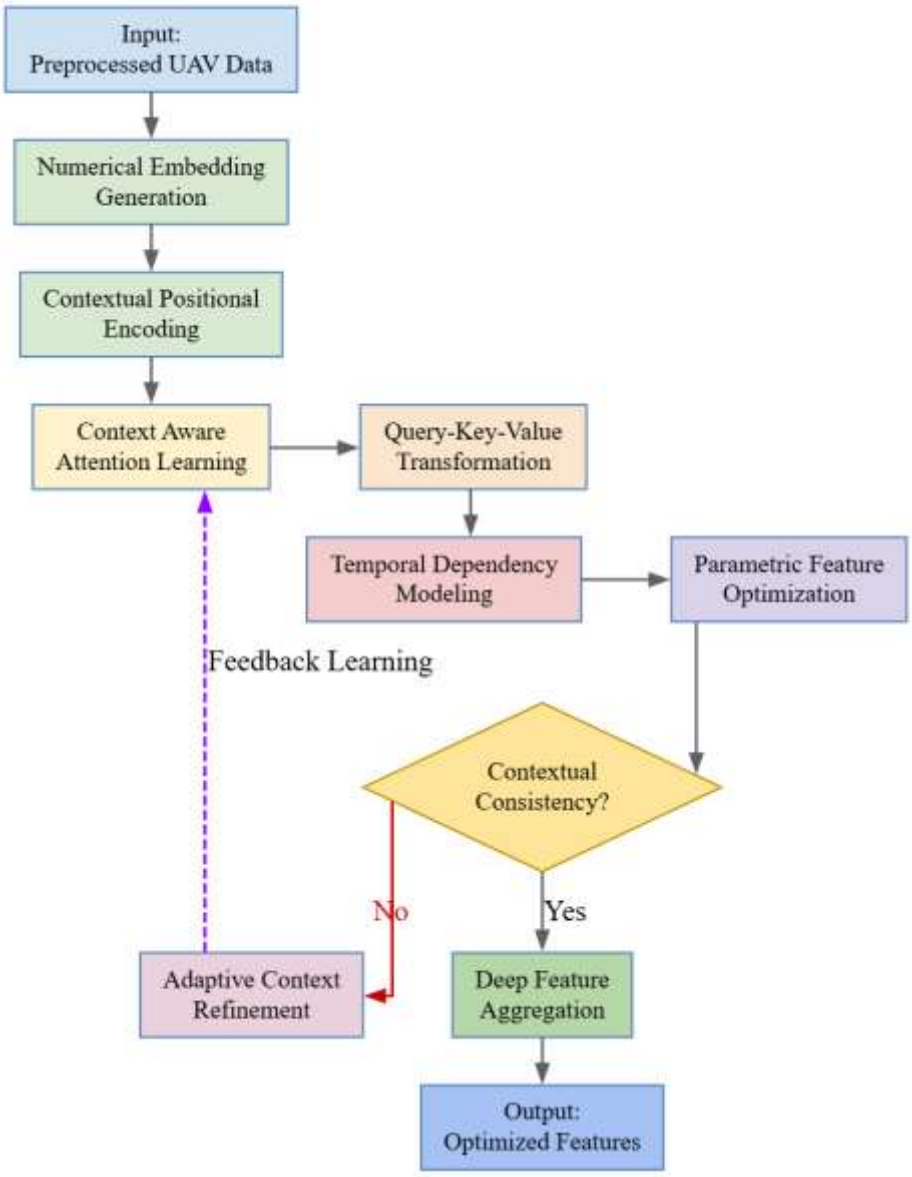

Figure 2. Proposed CAPN Transformer Feature Extraction Architecture.

3.2 GACN Classifier

The GACN classifier as presented in Figure 3 aims at intelligently categorizing UAV communication behavior by modelling complex relational dependencies among distributed fog-assisted network nodes. The main purpose of the GACN framework is to learn the structural interactions, communication flow dependencies, and contextual relationships from the extracted CAPN feature representations to find hidden cyber intrusion patterns. In contrast to traditional convolution or graph neural classifiers, the proposed GACN model combines graph convolution learning and adaptive attention mechanisms to dynamically highlight the links involved in communication that are more sensitive to security threats in UAV networks. The optimized contextual features obtained from the CAPN transformer are transformed into graph representations, where every UAV communication entity is represented as a graph node, and communication interactions are represented as graph edges. Then, the graph attention operations, neighborhood aggregation, adaptive weight updates, nonlinear feature propagation, and intrusion-sensitive node optimisation are done to catch the malicious communication behaviour. The learned graph embeddings are finally forwarded into the classification layer to classify the UAV traffic into Benign, DoS attacks and Replay attacks in an improved way with fewer false alarms. The obtained CAPN feature vectors are first encoded as graph node inputs:

$$G = (V, E) \tag{11}$$

10.48047/jocaaa.2020.28.06.15

In this case, Grepresents the graph structure of the communication behaviour of the UAVs. The set of graph nodes used to denote the UAV traffic instances is denoted as V, and communication edges between related network entities are denoted as E. This graph form allows for structural intrusion learning. The node feature matrix is created from contextual transformer outputs:

$$H^{(0)} = \{f_1, f_2, f_3, \dots, f_n\} \tag{12}$$

In this equation, $H^{(0)}$ is the initial node feature representation using CAPN feature extraction. Further, f_i represents the feature vector of the UAV communication node. This initialization keeps the sensitive numerical data from intrusions. The attention score between adjacent nodes is calculated as:

$$e_{ij} = \text{LeakyReLU}(a^T[Wh_i \parallel Wh_j]) \tag{13}$$

In this case, e_{ij} is the unnormalized attention score between the nodes i and j. Wdenotes the trainable transformation matrix and a^Tindicates the trainable attention weight vector. In this operation, the importance of communication between the UAV nodes is captured. The normalized attention importance is computed by using softmax activation:

$$\alpha_{ij} = \frac{\exp(e_{ij})}{\sum_{k \in N_i} \exp(e_{ik})} \tag{14}$$

Here, α_{ij} is the normalized attention coefficient of adjacent node interactions. The notation N_i restricts the neighbourhood set of node i. This normalisation process brings up some very significant communication relationships that are linked to attacks. The graph convolution propagation operation is represented by:

$$H^{(l+1)} = \sigma(\hat{A}H^{(l)}W^{(l)}) \tag{15}$$

In this case, $H^{(l+1)}$ is the updated node features at layer $l+1$. The $\hat{A}$represents normalized adjacency matrix and $W^{(l)}$represents convolution weights to be trained. This propagation operation is an aggregation of the surrounding information of UAV communication. The normalisation process by adjacency is expressed as:

$$\hat{A} = D^{-1/2}(A + I)D^{-1/2} \tag{16}$$

Here, Arepresents the adjacency matrix representing the connections between nodes in the UAV network graph. The matrix with diagonal elements equal to one, and off diagonal equal to zero, is called the Idenotes the identity matrix for self-loop preservation, and Dindicates the degree matrix. This normalization normalizes graph feature learning. Nonlinear activation function improves discriminative intrusion learning:

$$Z_i = \text{ReLU}(H_i) \tag{17}$$

Here $Z_i$denotes the activated graph feature representation for node i. The ReLU function adds nonlinearity by setting negative values of features to 0. This activation optimizes the discrimination of features that are vulnerable to attacks. The global graph feature aggregation is calculated:

$$G_f = \frac{1}{n}\sum_{i=1}^{n} Z_i \tag{18}$$

In this formulation, $G_f$represents the feature representation of the graph at the level of the graph, which is then aggregated for intrusion classification. Here, $n$denotes is a variable that is used to store the total number of graph nodes. In this aggregation operation, the overall UAV communication behavior is maintained. The classification probability distribution is created by softmax learning:

$$P(y_i) = \frac{e^{z_i}}{\sum_{c=1}^{C} e^{z_c}} \tag{19}$$

In this case, the probability of the ithattack class, $P(y_i)$ is the predicted probability. Here, z_i is the classifiers logits and C is the number of all intrusion categories. This operation is used to calculate the probability of Benign, DoS and Replay attacks. Next, the classification loss function is minimized for best intrusion prediction:

$$L = -\sum_{i=1}^{N} y_i \log(\hat{y}_i) \tag{20}$$

10.48047/jocaaa.2020.28.06.15

The cross-entropy classification loss that is minimized in the training of GACN is denoted as L in this equation. $y$are the actual class labels and $\hat{y}_i$is the predicted class probabilities. This optimization enhances the accuracy of classification and the reliability against intrusion.

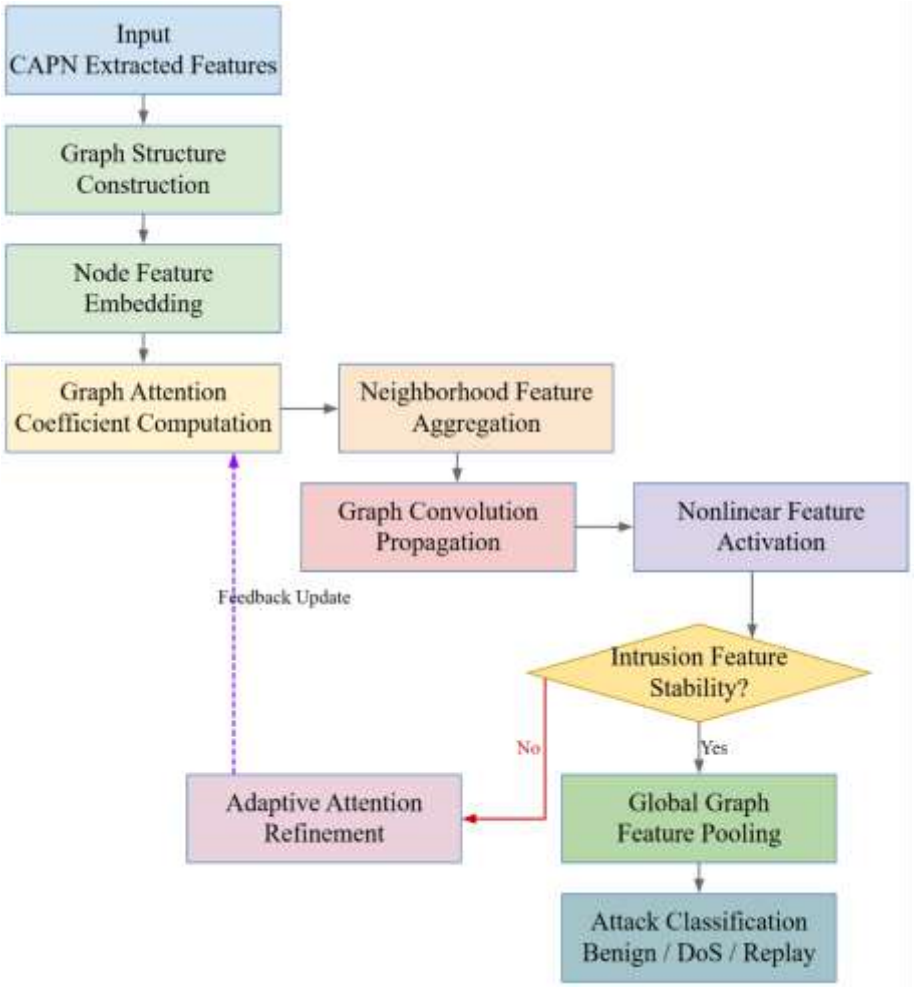

Figure 3. Proposed GACN Classifier Architecture.

4. Results and Discussion

In this section, a comprehensive comparison of several intrusion detection techniques is provided through comparison of their performance under the same experimental setup and UAV communication data set. The effectiveness, reliability and overall detection capability of each approach are analyzed using various evaluation metrics to assess the detection capabilities in fog-enabled UAV environments.

4.1 Dataset

UAV-NIDD is cyber-only version of the "Cyber-Physical Dataset for UAVs Under Normal Operations and Cyberattacks", which is refined by this study. This dataset is specifically tailored to enable efficient development of IDSs based on machine learning and deep learning techniques in an unmanned aerial vehicle communication environment, with the goal of only dealing with network-level cyberattack analysis. For pre-processing, all physical telemetry attributes were removed, and the categories (False Data Injection and Evil Twin) were removed to eliminate cyber-physical and infrastructure level dependencies. The last dataset only includes Benign, DoS and Replay traffic classes, corresponding to the normal traffic that a UAV send, DoS attacks and stealthy replay-based packet manipulation attacks respectively. Also, some attributes in the data set that were empty or lacked information were removed to make the data sets more consistent and to decrease the redundancy of attributes for more intrusion-focused analysis. The dataset description includes Wi-Fi WLAN communication features, frame-level network attributes, and timing-based traffic characteristics as well as the class column which is considered as the target label for the binary and multiclass classification problem. The dataset is very well suited for UAV

10.48047/jocaaa.2020.28.06.15

network intrusion detection, feature optimization, traffic behaviour analysis, benchmarking machine learning and deep learning models and lightweight IDS deployment in fog assisted UAV environment, due to its lightweight cyber-only structure. This repository is the original repository; it is available under the URL https://github.com/uamughal/UAVs-Dataset-Under-Normal-and-Cyberattacks.

4.2 Hyperparameters

The hyperparameter settings of the CAPN Transformer feature extraction as illustrated in Table 1 were carefully tuned for better contextual intrusion feature learning from UAV communication traffic. The learning rate was adjusted to be between 0.0001 and 0.01 with the best convergence performance at 0.001 for stable contextual learning. Number of batches from 16 to 128 were explored and 64 batches were found to be an efficient batch size in terms of memory usage and training performance. The embedding dimension varied from 32 to 512, and the best value of 128 was used to represent the numerical features of the data without causing significant computation overhead. Likewise, the model with 8 attention heads and 4 transformer layers performed better than the lower and deeper models in extracting contextual dependency. The dropout rate set at 0.3 prevented overfitting and retained the learning ability in general. An effective context window size was 16, which preserved temporal UAV communication relationships, and an activation slope of 0.10 leading to better nonlinear feature sensitivity. In addition, 100 training epochs and adding a weight decay of 0.0001 guaranteed stable optimization and higher accuracy of representation of features oriented to intrusion.

Table 1. Hyperparameter Settings for CAPN Transformer Feature Extraction.

Hyperparameter	Minimum Value	Maximum Value	Best Value
Learning Rate	0.0001	0.01	0.001
Batch Size	16	128	64
Embedding Dimension	32	512	128
Attention Heads	2	16	8
Transformer Layers	1	12	4
Dropout Rate	0.1	0.6	0.3
Context Window Size	4	64	16
Activation Function Slope	0.01	0.30	0.10
Epochs	10	300	100
Weight Decay	0.00001	0.001	0.0001

The hyperparameters of the GACN classifier as listed in Table 2 are optimized to represent the communication relationship among the UAVs in the fog computing environment. The graph learning rate was chosen within the range [0.0001, 0.01] with 0.001 converging the most successfully and providing stable graph attention learning performance. The depth of GACN varied from 1 to 10 layers, and the three-layer GACN achieved optimal performance in terms of graph feature propagation and computational efficiency. The number of layers in the GACN was varied from 1 to 10 layers, with the three-layer GACN showing the best performance in terms of feature propagation and computational efficiency. Hidden units from 16 to 512 were explored and 128 hidden units produced highly discriminative representations of intrusion. To prevent overfitting in learning node relationships, the optimal graph attention performance was obtained with a graph dropout rate of 0.4 and 8 attention coefficients. The neighborhood aggregation size of 8 enhanced UAV structural communication dependency extraction. Also, a graph batch size of 32, activation threshold of 0.5, and classification threshold of 0.5 improved the consistency of attack classification. Finally, 150 training epochs were used, which led to a stable convergence of the graphs and resulted in the improvement of detection performance for Benign, DoS and Replay attacks.

10.48047/jocaaa.2020.28.06.15

Table 2. Hyperparameter Settings for GACN Classifier.

Hyperparameter	Minimum Value	Maximum Value	Best Value
Graph Learning Rate	0.0001	0.01	0.001
Number of GACN Layers	1	10	3
Hidden Units	16	512	128
Attention Coefficients	2	16	8
Graph Dropout Rate	0.1	0.7	0.4
Neighbor Aggregation Size	2	20	8
Graph Batch Size	8	128	32
Activation Threshold	0.1	1.0	0.5
Training Epochs	20	500	150
Classification Threshold	0.3	0.9	0.5

4.3 Performance Analysis

A comparison of the proposed CAPN-GACN framework with other hybrid deep learning-based ID models that have already been proposed for UAV cybersecurity applications is shown in Table 3. The MLDL model achieved the following performance with an accuracy of 97.68%, precision of 97.11%, recall of 96.92%, and F1-score of 97.01%, with good intrusion detection baseline performance. In the same way, the ST-GNN framework [11] enhanced the overall detection capability with 98.04% accuracy, 97.82% precision, 97.55% recall, and 97.68% F1-score with the help of spatio-temporal graph learning mechanisms. The AdvGAN model [14] improved the model's attack detection capability, with adversarial intrusion learning yielding 98.73% accuracy, 98.44% precision, 98.12% recall and 98.28% F1-score. Furthermore, the LTS-Transformer model [15] gave better hybrid learning performance with 99.11% accuracy, 98.92% precision, 98.74% recall, and 98.83% F1-score in performing lightweight temporal-spatial transformer analysis. The proposed CAPN-GACN framework presented the best accuracy, 99.91%, for intelligent UAV cyber intrusion detection, which was significantly higher than all the existing hybrid deep learning schemes, with the precision and recall reaching 99.88% and 99.84% respectively and the F1-score of 99.86%, showing the superior capability of contextual parametric transformer learning and graph attention convolution modeling to deal with intelligent UAV cyber intrusion detection.

Table 4 shows the proposed UAV-FC-CIDS framework with some of the existing federated AI-based IDSs for UAV network security. The GenFed-IDS framework achieved a moderate level of intrusion detection with accuracy of 94.82%, precision of 94.11%, recall of 93.76% and F1-score of 93.93% in federated UAV environment. Similarly, the FGNN-DTCN-LSTM model [13] outperformed it in terms of accuracy (95.47%), precision (95.08%), recall (94.66%), and F1-score (94.87%) using graph neural networks, temporal convolution, and LSTM learning. The performance of intrusion classification was further enhanced by the sequential deep learning analysis of RoboLSTM-IDS framework with 97.14% accuracy, 96.88% precision, 96.41% recall and 96.64% F1-score. In the similar fashion, the BRFL-ViT model [12] has demonstrated a 98.26% accuracy, 97.92% precision, 97.66% recall, and 97.79% F1-score with the help of Byzantine-robust federated transformer learning. However, the overall accuracy of 99.83%, precision of 99.76%, and recall of 99.71%, coupled with an F1-score of 99.73%, validated the superiority of the proposed UAV-FC-CIDS model in terms of overall performance in the context of fog-enabled UAV cybersecurity applications, including the proposed contextual transformer and graph attention-based intrusion detection architecture.

Table 3. Performance Comparison with Hybrid Deep Learning Classifiers.

Method	Accuracy (%)	Precision (%)	Recall (%)	F1 Score (%)

10.48047/jocaaa.2020.28.06.15

MLDL [10]	97.68	97.11	96.92	97.01
ST-GNN [11]	98.04	97.82	97.55	97.68
AdvGAN [14]	98.73	98.44	98.12	98.28
LTS- Transformer [15]	99.11	98.92	98.74	98.83
Proposed CAPN GACN	99.91	99.88	99.84	99.86

Table 4. Performance Comparison with Federated AI based IDS Systems.

Method	Accuracy (%)	Precision (%)	Recall (%)	F1 Score (%)
GenFed-IDS [9]	94.82	94.11	93.76	93.93
FGNN -DTCN-LSTM [13]	95.47	95.08	94.66	94.87
RoboLSTM-IDS [20]	97.14	96.88	96.41	96.64
BRFL-ViT [12]	98.26	97.92	97.66	97.79
Proposed UAV-FC-CIDS	99.83	99.76	99.71	99.73

4.4 Discussions

Table 5 shows the computational complexity of different UAV intrusion detection techniques with respect to training time, testing time and memory usage. The GenFed-IDS model [9] took 68.4 minutes to train, 3.91 seconds to test, and 742 MB of memory, which implies moderate computational ability in the federated intrusion detection of UAVs. The graph neural network framework FGNN-DTCN-LSTM [13] also added a significant amount of computational overhead: 81.7 minutes of training time, 4.82 seconds of testing time, and a usage of 896 MB of memory, because of incorporating graph neural and temporal learning operations. The RoboLSTM-IDS model [20] had the largest computational cost with training time of 95.3 minutes, test time of 5.67 seconds and consumed 1048 MB memory due to its deep sequential learning approach. The proposed CAPN-GACN framework outperform the other methods in terms of computational efficiency, requiring the shortest training time of 52.6 minutes and testing time of 2.14 seconds, as well as the smallest memory of 618 MB, showing that the proposed contextual transformer and graph attention network learning framework not only enables early detection of attacks in real time in a fog-enabled UAV cybersecurity environment, but also uses less memory and requires fewer training time and resources.

To assess the contribution of each component in overall intrusion detection performance, the ablation study of the proposed UAV-FC-CIDS framework has been performed using various alternative combinations of models as shown in Table 6. In the model without CAPN Transformer, the accuracy was 96.88%, the precision was 96.41%, the recall was 96.12%, and the F1-score was 96.26%, indicating that contextual transformer learning plays a significant role in enhancing feature discrimination capability. Similarly, after removing the GACN classifier, the accuracy increased to 97.24%, precision to 96.93%, recall to 96.74%, and F1 score to 96.83%, but still lacked the ability to handle structural graph relationships well. The Transformer model with GCN model achieved 98.64% accuracy, 98.27% precision, 98.04% recall, and 98.15% F1-score, and the CAPN model with DNN network achieved 98.11% accuracy, 97.82% precision, 97.51% recall, and 97.66% F1-score, respectively, which shows the importance of combining contextual and graph-based learning mechanism. The CAPN with CNN-LSTM model also achieved 99.08% accuracy, 98.84% precision, 98.62% recall and 98.73% F1-score with better sequential feature learning performance. The overall performance of the full proposed UAV-FC-CIDS framework was the best with 99.91% accuracy, 99.88% precision, 99.84% recall, and 99.86% F1-score, which verify the effectiveness of the proposed integration of CAPN Transformer feature extraction and GACN classification in the intelligent UAV cyber intrusion detection field.

Table 5. Computational Complexity Comparison of Various Methodologies.

10.48047/jocaaa.2020.28.06.15

Method	Training Time (min)	Testing Time (sec)	Memory Usage (MB)
GenFed-IDS [9]	68.4	3.91	742
FGNN -DTCN-LSTM [13]	81.7	4.82	896
RoboLSTM-IDS [20]	95.3	5.67	1048
Proposed CAPN GACN	52.6	2.14	618

Table 6. Ablation Study of Proposed UAV-FC-CIDS Framework with Alternative Components.

Model Variation	Accuracy (%)	Precision (%)	Recall (%)	F1 Score (%)
Without CAPN Transformer	96.88	96.41	96.12	96.26
Without GACN Classifier	97.24	96.93	96.74	96.83
CAPN With DNN	98.11	97.82	97.51	97.66
Transformer With GCN	98.64	98.27	98.04	98.15
CAPN With CNN LSTM	99.08	98.84	98.62	98.73
Full Model	99.91	99.88	99.84	99.86

5. Conclusion

The framework of UAV-FC-CIDS was designed and developed successfully, which introduces a novel cyber intrusion detection architecture for fog communication environments based on UAV. The proposed hybrid framework well represented the dependencies among contextual communications, temporal traffic characteristics, and graph-based structural attack relationships of the UAV network traffic, which enabled accurate identification of Benign, DoS and Replay attacks. Experimental results showed that the proposed model outperformed the current hybrid deep learning and federated AI based IDSs with 99.91% accuracy, 99.88% precision, 99.84% recall and 99.86% F1-score. Moreover, the framework had advantages in terms of computational efficiency, training times of 52.6 minutes, testing times of 2.14 seconds, and using only 618 MB of memory were suitable for a real-time UAV fog computing environment. The ablation study also confirmed the effectiveness of the contextual learning of CAPN Transformer combined with the graph attention classification of GACN in providing robust and scalable UAV cybersecurity protection. The proposed framework can be further extended towards multi-UAV collaborative intrusion detection, prediction of zero-day attacks, federated edge intelligence, explainable AI-driven cybersecurity analysis and lightweight deployment on resource-constrained aerial communication platforms in future research. Furthermore, the incorporation of blockchain technology-enabled secure communication protocols and quantum-resistant cyber-security systems could contribute to the more robust reliability, privacy safeguarding, and robustness of intelligent UAV fog computing systems against emerging cyber threats.

References

[1]. Mkiramweni, Mbazingwa Elirehema, Chungang Yang, Jiandong Li, and Wei Zhang. "A survey of game theory in unmanned aerial vehicles communications." *IEEE Communications Surveys & Tutorials* 21, no. 4 (2019): 3386-3416.

[2]. Dahiya, Susheela, and Manik Garg. "Unmanned aerial vehicles: Vulnerability to cyber attacks." In *International Conference on Unmanned Aerial System in Geomatics*, pp. 201-211. Cham: Springer International Publishing, 2019.

[3]. Shakhatreh, Hazim, Ahmad H. Sawalmeh, Ala Al-Fuqaha, Zuochao Dou, Eyad Almaita, Issa Khalil, Noor Shamsiah Othman, Abdallah Khreishah, and Mohsen Guizani. "Unmanned aerial vehicles (UAVs): A survey on civil applications and key research challenges." *IEEE access* 7 (2019): 48572-48634.

10.48047/jocaaa.2020.28.06.15

[4]. García-Magariño, Iván, Raquel Lacuesta, Muttukrishnan Rajarajan, and Jaime Lloret. "Security in networks of unmanned aerial vehicles for surveillance with an agent-based approach inspired by the principles of blockchain." *Ad Hoc Networks* 86 (2019): 72-82.

[5]. Cebeloglu, F. Sumeyye, and Mehmet Karakose. "A cyber security analysis used for unmanned aerial vehicles in the smart city." In *2019 1st International Informatics and Software Engineering Conference (UBMYK)*, pp. 1-6. IEEE, 2019.

[6]. Kim, Eui-Jin, Ho-Chul Park, Seung-Woo Ham, Seung-Young Kho, and Dong-Kyu Kim. "Extracting vehicle trajectories using unmanned aerial vehicles in congested traffic conditions." *Journal of Advanced Transportation* 2019, no. 1 (2019): 9060797.

[7]. Dhulkefl, Elaf Jirjees, and Akif Durdu. "Path planning algorithms for unmanned aerial vehicles." *Int. J. Trend Sci. Res. Dev* 3, no. 4 (2019): 359-362.

[8]. Tan, Xiaopeng, Shaojing Su, Zhen Zuo, Xiaojun Guo, and Xiaoyong Sun. "Intrusion detection of UAVs based on the deep belief network optimized by PSO." *Sensors* 19, no. 24 (2019): 5529.

[9]. Ferrag, Mohamed Amine, and Leandros Maglaras. "DeliveryCoin: An IDS and blockchain-based delivery framework for drone-delivered services." *Computers* 8, no. 3 (2019): 58.

[10]. Arthur, M. P. (2019, August). Detecting signal spoofing and jamming attacks in UAV networks using a lightweight IDS. In *2019 international conference on computer, information and telecommunication systems (CITS)* (pp. 1-5). IEEE.

[11]. Condomines, Jean-Philippe, Ruohao Zhang, and Nicolas Larrieu. "Network intrusion detection system for UAV ad-hoc communication: From methodology design to real test validation." *Ad Hoc Networks* 90 (2019): 101759.

[12]. Ghubaish, Ali, Tara Salman, and Raj Jain. "Experiments with a LoRaWAN-Based Remote ID System for Locating Unmanned Aerial Vehicles (UAVs)." *Wireless Communications and Mobile Computing* 2019, no. 1 (2019): 9060121.

[13]. Khan, Samir, Chun Fui Liew, Takehisa Yairi, and Richard McWilliam. "Unsupervised anomaly detection in unmanned aerial vehicles." *Applied Soft Computing* 83 (2019): 105650.

[14]. Xie, Zhengyu, and Yong Qin. "High-speed railway perimeter intrusion detection approach based on Internet of Things." *Advances in Mechanical Engineering* 11, no. 2 (2019): 1687814018821511.

[15]. Li, Xinghua, Yunwei Wang, Pandi Vijayakumar, Debiao He, Neeraj Kumar, and Jianfeng Ma. "Blockchain-based mutual-healing group key distribution scheme in unmanned aerial vehicles ad-hoc network." *IEEE Transactions on Vehicular Technology* 68, no. 11 (2019): 11309-11322.

[16]. Yang, Ting, Chuan Heng Foh, Fabien Heliot, Chee Yen Leow, and Periklis Chatzimisios. "Self-organization drone-based unmanned aerial vehicles (UAV) networks." In *ICC 2019-2019 IEEE International Conference on Communications (ICC)*, pp. 1-6. IEEE, 2019.

[17]. Yu, Ziquan, Yaohong Qu, and Youmin Zhang. "Fault-tolerant containment control of multiple unmanned aerial vehicles based on distributed sliding-mode observer." *Journal of Intelligent & Robotic Systems* 93, no. 1 (2019): 163-177.

[18]. Haque, Md Samsul, and Morshed U. Chowdhury. "Ad-hoc framework for efficient network security for unmanned aerial vehicles (UAV)." In *International Conference on Future Network Systems and Security*, pp. 23-36. Cham: Springer International Publishing, 2019.

[19]. Jena, Kalyan Kumar, Sourav Kumar Bhoi, Bhruti Dipta Behera, Subhasis Panda, Bandana Sahu, and Rutuwi Sahu. "A trust based false message detection model for multi-unmanned aerial vehicle network." In *2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, pp. 324-329. IEEE, 2019.

[20]. Haque, Md Samsul, and Morshed U. Chowdhury. "Ad-hoc framework for efficient network security for unmanned aerial vehicles (UAV)." In *International Conference on Future Network Systems and Security*, pp. 23-36. Cham: Springer International Publishing, 2019.