Adaptive Neuro-Fuzzy Inference System-based Lightweight Intrusion Detection System for UAVs

Alvi Ataur Khalil* and Mohammad Ashiqur Rahman†
*†Electrical and Computer Engineering, Florida International University, USA
†Knight Foundation School of Computing and Information Sciences, Florida International University, USA
*akhal042@fiu.edu, †marahman@fiu.edu

***Abstract*—Unmanned aerial vehicles (UAVs) are widely utilized in myriad domains due to their low infrastructure cost and flexibility in deployment. Hostile and unsafe networking environments can make UAVs vulnerable to various attacks. Intrusion detection systems (IDSs) have been developed to detect such attacks. However, conventional data-driven IDSs can be architecturally complex and computationally intensive for resource-constrained small UAVs. In this work, we propose a lightweight IDS for UAVs leveraging an adaptive neuro-fuzzy inference system (ANFIS) that combines artificial neural networks (ANNs) and fuzzy deduction frameworks. Due to the simplistic membership and rule-based classification capabilities of ANFIS, our proposed IDS is lightweight and perfectly suitable for small UAVs. We evaluate the ANFIS-IDS's effectiveness by comparing its performance to conventional data-driven classification models. In particular, we contrast the proposed IDS with a traditional novelty-based IDS for UAV sensor attacks. We further compare their deployment in a hardware-emulated UAV testbed, assessing the proposed model's lightweight nature.**

***Index Terms*—Fuzzy Inference, Membership function, ANN, ANFIS, Intrusion detection system**

I. Introduction

Unmanned aerial vehicles (UAVs) have been demonstrated to be a prominent tool for various applications, including monitoring of industrial control systems, law enforcement, military operations, etc. [1]–[7]. However, some of these application domains are potentially insecure from a networking perspective, leaving UAVs vulnerable to various attacks. To ensure reliable and trustworthy information transfer between network components, it is necessary to protect these devices against intrusion attempts [8]. Intrusion detection systems (IDSs) have been developed to detect various kinds of attacks in networked UAV control [9], [10].

The majority of anomaly detection techniques currently used in the UAV industry are predictive models that analyze and predict sensor readings. The most popular models include autoregressive models, linear dynamic state space models, and neural network-based regression models. However, the computational complexity of these models often questions their feasibility in the UAV domain. Fuzzy logic, on the other hand, is much simpler and yet closely resembles human reasoning and decision-making. In applications where the relationships between inputs and outputs are complex, nonlinear, or difficult to model using traditional mathematical equations, adaptive neuro-fuzzy inference system (ANFIS) has become a very useful tool due to its nonlinear interaction designs, variational flexibility, and rapid learning limits [11]. It is a hybrid artificial intelligence system combining the advantages of artificial neural networks (ANNs) with fuzzy deduction frameworks. It works by learning a set of fuzzy if-then rules from input-output data using a training algorithm such as backpropagation. Then, it uses these learned rules to make predictions or decisions based on new input data. Therefore, ANFIS has become an excellent tool for prediction and classification problems, including cyber attack detection in various application domains [12].

Small UAVs are edge devices with constrained resources like processing power, memory, and battery life, which can quickly be overwhelmed if loaded with heavyweight security solutions [13]. Hence, for detecting intrusions in UAV networks, lightweight IDS, requiring minimal computational resources, are essential [14]. The existing works in the literature construct IDS for UAVs by utilizing machine learning (ML) models, which incorporate network parameters to detect intrusions. However, the size of these IDS can become significantly large, making it impractical to deploy the model in resource-constrained small UAV domains.

In this work, we propose an ANFIS-based IDS that is tailored for the domain of networked UAVs. The proposed IDS is capable of detecting intrusions in the communication channel of UAVs using simple membership functions and logical operations that combine to generate classification rules. Compared to the ML-based models, ANFIS-IDS provides a lightweight solution that is ideal for small UAVs, conventionally equipped with limited resources. The lightweight nature of the proposed IDS is achieved by using a fuzzy inference system, which provides a more straightforward and less computationally intensive solution compared to complex machine learning algorithms. To the best of our knowledge, this paper is the first to propose the use of ANFIS-based IDS for UAV networks. To evaluate the effectiveness of the proposed ANFIS-IDS, the paper uses standard performance metrics to compare it with conventional classification models. The results show that the proposed IDS achieves similar or better performance than these models, despite its lightweight design. Furthermore, to demonstrate the practicality of the proposed IDS, the paper deploys it in a real hardware-emulated UAV testbed. The results of this test demonstrate the ability of the IDS to effectively detect intrusions in UAV communication channels while running on hardware with limited resources.

Key contributions of this work are three-fold:

- Designed and implemented an ANFIS-based IDS for UAV communication systems that can effectively detect GPS spoofing and jamming attacks.
- The IDS's performance is assessed by comparing its accuracy metrics with conventional data-driven classification models. Additionally, its effectiveness is verified by contrasting it with the novelty-based IDS for UAV sensor attacks [15].
- Both the novelty-based IDS and ANFIS IDS are deployed in a real hardware-emulated UAV testbed, which is a resource-constrained environment, to evaluate the lightweight nature of the proposed model.

The succeeding sections are arranged as follows: Required preliminary information is briefly presented in Section II. Section III discusses the related research works. The proposed framework is presented in Section IV. The technical specifics are discussed in Section V. In Section VI, the evaluation setup is presented along with the empirical analysis and findings. Finally, the paper is concluded with Section VII.

II. Background

This section presents some preliminary concepts related to the proposed IDS.

A. Intrusion Detection Systems

Intrusion detection refers to the techniques that can identify interference and security assaults and is used in the context of data security. The literature has presented a number of intrusion detection systems (IDSs) that employ a variety of algorithms and strategies in an effort to find intrusions and anomalies [16]. The cutting-edge IDSs can be broadly categorized into three groups: knowledge-based techniques, model-based techniques, and data-driven techniques [17]. To efficiently detect intrusions, the first two methods need to comprehend the domain knowledge or system mechanism. However, for many real-world domains, such as UAV control, it is typically difficult to develop an accurate physical model [18]. The data-driven approaches, on the other hand, automatically learn the behavioral model of the system based on gathered system data. Consequently, we present a data-driven IDS in this work.

B. ANFIS

ANFIS is a unique type of ANN that combines the principles of fuzzy logic and neural networks to create a hybrid system capable of performing both symbolic and numerical computations. This powerful inference system employs IF-THEN rules to modify a nonlinear function, which allows it to act as an effective and ideal estimator, as demonstrated in various studies [19], [20]. ANFIS has found success in numerous fields, such as engineering, medicine, finance, and robotics, among others, due to its ability to learn from data and adapt to changing conditions, making it an excellent tool for modeling complex systems. Utilizing given input/output data, ANFIS can create mapping based on both human knowledge,

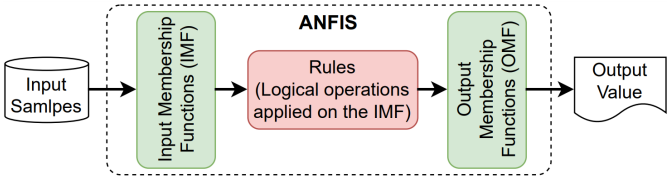


Fig. 1. Workflow of input-output mapping in ANFIS.

in the form of fuzzy if-then rules, and neural learning algorithms [21]. The workflow of ANFIS's input-output mapping is presented in Fig. 1, where two set membership functions (input and output) along with a set of logical operations (forming rules) dictate the estimation task. One of the significant attributes of ANFIS is its ability to represent complex relations among the neurons of ANNs through a combination of simple conditions. This makes ANFIS a valuable tool for applications that require complex modeling and analysis of data.

III. Related Works

This section presents the literature review of related domains. There are various fuzzy IDS techniques published in the literature. For instance, Chandrasekhar et al. described a method for intrusion detection [22] that first performs initial clustering and then goes on to train the fuzzy ANN model using radial support vector machine (SVM) classifiers and fuzzy-ANN. The SVM vectors are then created, and the radial SVM is used for the final classification. An instance selection approach is suggested in Ashfaq et al. [23] to enhance the training of data using fuzzy logic. For each training set of data, they created a membership vector by using the randomized weighted neural network (RWNN) as a basis classifier. To increase the detection rate and stability of the IDS, Lei et al. used an ANN and fuzzy sets [24]. However, the necessary techniques for training and improving the ANN are not specified. Karaboga et al. proposed an artificial bee colony algorithm for ANFIS classifier training in [25]. In this algorithm, the mechanism for producing solutions is based on the adaptivity value that was created using the failure counter and the crossover operator. The IDS technique proposed by Ganeshkumar et al. [26] offers a hypervisor detector, an IDS created to function at the hypervisor layer. It is created using ANFIS and implemented using a hybrid strategy that combines the least squares method and the backpropagation gradient descent method. Sajith et al. proposed a network IDS using an ANFIS classifier to detect and classify different types of network intrusions [11]. The IDS outperformed other classifiers in accuracy and detection rate using the KDD Cup 1999 dataset. Moudni proposed a fuzzy-based IDS for detecting black hole attacks in MANETs [27], which utilizes the Mamdani fuzzy inference system to identify black hole attacks based on routing information. The proposed system was evaluated using NS-2 and demonstrated high accuracy in detecting attacks.

None of the above-mentioned works, however, have focused on intrusion attacks such as GPS spoofing and jamming in UAV control networks. ANFIS-based IDS is particularly

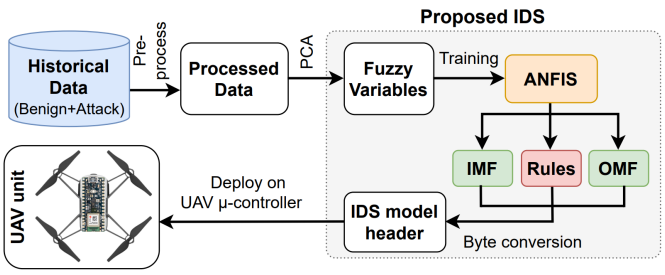


Fig. 2. Framework of the proposed ANFIS-based IDS.

crucial for resource-constrained devices like small UAVs due to its lightweight attribute. However, in the existing literature, IDSs for the UAV domain are mostly based on ML models, which are usually computationally expensive [28]–[30]. Although ML-based IDSs have several advantages over traditional signature-based IDSs, their deployment often becomes infeasible in resource-constrained UAV units. We fill up this research gap by proposing the ANFIS-IDS for UAVs.

IV. Framework

We introduce our proposed ANFIS-based IDS in this section. As shown in Fig. 2, the IDS requires historical data (including both benign and attack samples) to be trained, in order to accurately identify and detect UAV network intrusions. This aspect of the proposed IDS is similar to conventional ML-based IDSs, however, the crucial difference is the final model that is trained and deployed in the UAV hardware.

Before feeding into the IDS, the data is processed and reduced through two sequential steps. First, the preprocessing is done through merging different sensor data, scaling the data, and dropping features with minimal correlation with the target label. Then we perform principal component analysis (PCA) [31] to further reduce the dimensionality of the feature space. The reason behind performing PCA is to reduce the training sample space to an order that will make sure the IDS performs reasonably well while the underlying model does not become too complex. We experiment with different percentages of variance and advocate capturing 70% variance to maintain detection accuracy. Then the final data is fed to the IDS as input and ANFIS generates input membership functions (IMFs) for each of the input components. Then different logical operations are performed among the IMFs to generate the rules that will dictate the decision of the IDS. The results of each rule are mapped into output membership functions (OMFs), which are aggregated to generate an output. These three components (IMFs, Rules, OMFs) define the proposed ANFIS-IDS, which are converted into byte code to generate the header file of the IDS. Finally, the machine-executable model is deployed on the microcontroller of a UAV.

V. Technical Details

This section presents the technical details of the proposed IDS model. First, the underlying fuzzy inference system

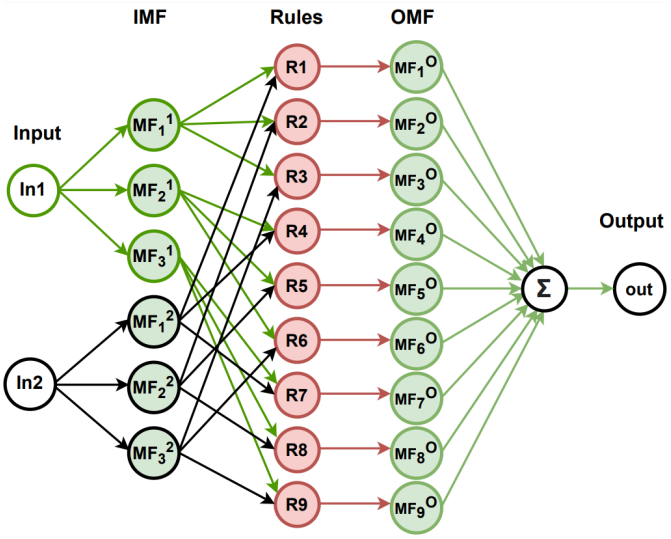


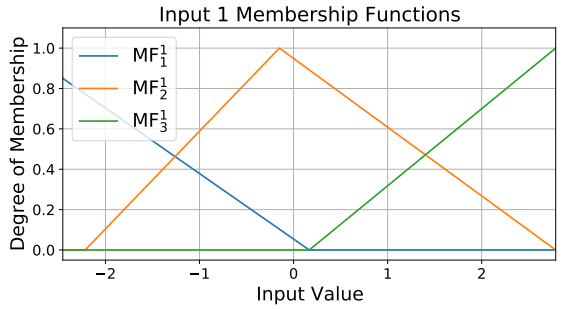
Fig. 3. Neural structure of the proposed ANFIS-based IDS.

(Takagi-Sugeno-Kang) has been discussed briefly. Then, the structure and processing of the data are presented. Afterward, the modeling of the ANFIS-IDS is demonstrated, followed by the generated rules. Finally, a case study is shown for a particular set of input patterns along with computed labels.

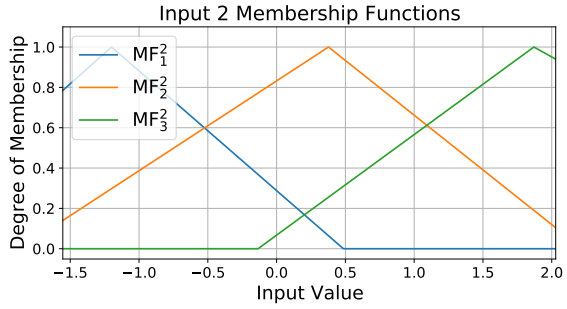
A. Takagi-Sugeno-Kang Fuzzy Inference System

We utilize the Takagi-Sugeno-Kang (TSK) fuzzy inference system in our IDS model. TSK is a powerful rule-based system that is commonly used in various fields, including information security. In an IDS model, TSK is used to infer a fuzzy output label based on a set of fuzzy input patterns. First, input variables are fuzzified into fuzzy sets to determine the membership degree of the input variables in each set. The membership degree of an input variable in a fuzzy set indicates the degree to which the input variable belongs to the set. Next, fuzzy rules are applied to these fuzzy sets to generate fuzzy output values. These rules are typically represented as "IF-THEN" statements, where the "IF" part contains a set of conditions, and the "THEN" part contains a set of conclusions. Each rule corresponds to a specific decision boundary, and the model's parameters can be interpreted as the weights of the decision boundary. Finally, the crisp output value is obtained by defuzzifying the fuzzy output values. Defuzzification is the process of converting a fuzzy output value into a crisp value. This process involves weighing the contribution of each fuzzy set to the overall output value.

One of the significant advantages of the TSK fuzzy inference system is its high interpretability [32]. The TSK model's rules are easy to understand, and each rule corresponds to a specific decision boundary. In addition, TSK is highly accurate and can be used efficiently for classification applications [33]. Overall, the TSK fuzzy inference system is a powerful tool for developing IDS models. Its ability to handle uncertainty and imprecision in data, combined with its high accuracy and



(a)



(b)

Fig. 4. The membership function plots for (a) the first input variable and (b) the second input variable, of the ANFIS-IDS.

interpretability, makes it a very powerful tool for intrusion detection tasks [34].

B. Data Processing

Similar to ML models, ANFIS also gets trained on historical data to predict/classify future unknown data. We utilized the UAV flight dataset available at [35], which includes three types of flight data:

- **Flights with GPS spoofing:** A Great Scott Gadgets HackRF software-defined radio is used with the GPS-SDR-SIM tool to broadcast 30.286502,120.032669.
- **Flights with GPS jamming:** Done by broadcasting white gaussian noise using the HackRF, with an amplitude of 0.3 and a gain of -48dB.
- **Benign Flight:** No attacks attempted.

The data set available at [35] had more than 25k samples and each sample has 1050 features, from where we dropped the features that have very low correlation with the label. Then the missing data is filled up with average column values. Finally, we dropped columns having the same value for all the samples and used the training slice of the dataset to train five classification models (discussed later in Section VI). Then for the ANFIS-based IDS, we performed PCA to improve the data's interpretability while retaining the most information possible. We set the PCA parameters to retain 70% of the total variance and ended up with two input features (2 principal components). We used that data set along with the label column to train the ANFIS model.

C. Modeling ANFIS

We utilized the Matlab Fuzzy Logic Toolbox for modeling the ANFIS-IDS. The neural structure of the proposed TSK network is presented in Fig. 3, where MF_i^j presents the i-th membership function of the j-th input (i.e., PCj), RK presents the K-th rule, and MF_i^O presents the i-th output membership function. According to the processed input set, we have two input processing elements (PEs) in the first layer, each passing one principal component (PC). We set three membership functions for each input value, which are adapted through gradient updates during the training phase. The resultant final membership function for input one and input two are presented in Fig. 4(a) and Fig. 4(b), respectively. We set the number of rules to nine, where each rule is a logical combination of a pair of membership functions. The toolbox generated the logical combinations according to the mapping of the input features to the output label. A firing weight and consequent value are generated at each rule according to the input values and membership degrees.

TABLE I
RULES OF ANFIS-IDS

Rule	***PC1***	***PC2***	***Output***
R1	Small, MF_1^1	Small, MF_1^2	Jam, min(MF_1^1, MF_1^2)
R2	Small, MF_1^1	Medium, MF_2^2	Spoof, min(MF_1^1, MF_2^2)
R3	Small, MF_1^1	Large, MF_3^2	Spoof, min(MF_1^1, MF_3^2)
R4	Medium, MF_2^1	Small, MF_1^2	Jam, min(MF_2^1, MF_1^2)
R5	Medium, MF_2^1	Medium, MF_2^2	Benign, min(MF_2^1, MF_2^2)
R6	Medium, MF_2^1	Large, MF_3^2	Spoof, min(MF_2^1, MF_3^2)
R7	Large, MF_3^1	Small, MF_1^2	Benign, min(MF_3^1, MF_1^2)
R8	Large, MF_3^1	Medium, MF_2^2	Benign, min(MF_3^1, MF_2^2)
R9	Large, MF_3^1	Large, MF_3^2	Benign, min(MF_3^1, MF_3^2)

Finally, all the consequent values from the nine rules are aggregated according to the firing weight to generate the final output. The final layer has only one PE, which represents the predicted label for the given input sample. The output PE can have three different values, representing the benign, the GPS spoofing, and the GPS jamming signal, respectively. The generated membership functions for inputs are as follows:

Input 1: Takes in the value of Principal Component 1 (PC1), which ranges from -2.4537 to 2.7874.

- Small: If the value is between -2.4537 to 0.167. In Fig. 4(a), MF_1^1 presents this membership.
- Medium: If the value is between -2.2158 to 2.7874. In Fig. 4(a), MF_2^1 presents this membership.
- Large: If the value is between 0.167 to 2.7874. In Fig. 4(a), MF_3^1 presents this membership.

Input 2: Takes in the value of Principal Component 2 (PC2), which ranges from -1.5541 to 2.0288.

- Small: If the value is between -1.5541 to 0.4856. In Fig. 4(b), MF_1^2 presents this membership.
- Medium: If the value is between -1.5541 to 2.0288. In Fig. 4(b), MF_2^2 presents this membership.
- Large: If the value is between -0.0874 to 2.0288. In Fig. 4(b), MF_3^2 presents this membership.

Each ANFIS-generated rule performs a logical operation on the input values to generate an output consequent and a

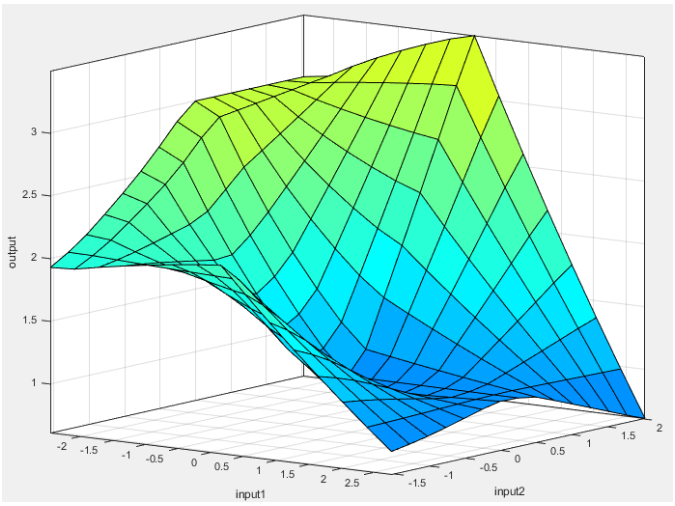


Fig. 5. Rules Surface for the ANFIS-based IDS.

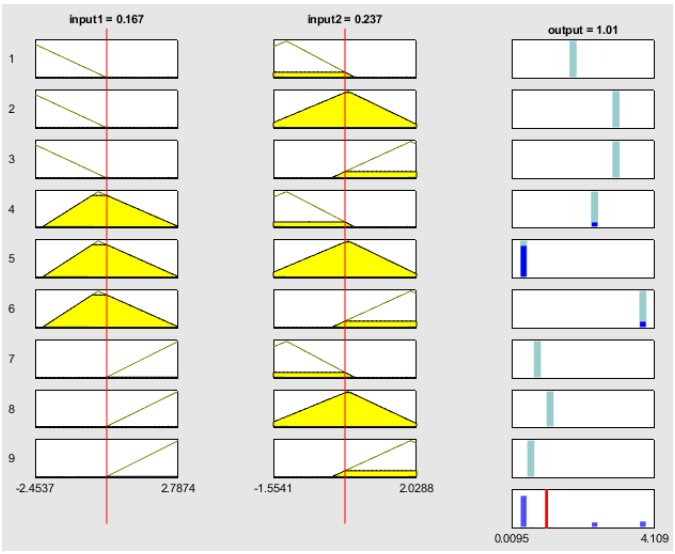


Fig. 6. Case study for two specific input values (0.167 and 0.237) and corresponding output value/label (1.01).

firing weight (degree of output membership function). Table I summarizes all nine rules.

The generated rules surface is presented in Fig. 5, where the horizontal axis-es represent the values of the two inputs and the vertical axis represents the variable output value. Based on the surface figure, it is evident that there are no three separate flat surfaces, resembling staircases, for the three labels. Instead, we observe minor variations around the values of 1, 2, and 3. Consequently, to determine the actual label for a sample, we round the output value to the closest integer.

D. Case Study

We present a case study in Fig. 6 (screenshot from ANFIS toolbox) for a particular set of input values. The PC1 and PC2 are set to 0.167 and 0.237, respectively. We observe that $R5$ achieves the highest firing weight since both the inputs have

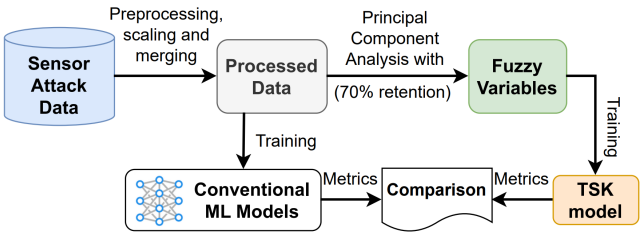


Fig. 7. Experimental Methodology.

a high degree of membership in the respective membership functions (MF_2^1, MF_2^2) of $R5$. Among others, $R4$ and $R6$ have very low firing weights, while the rest has negligible weights. After aggregation, we observe the final output as 1 (after rounding the actual output of 1.01), meaning the corresponding input sample is detected as benign.

VI. Experiments and Discussions

In this section, we analyze and evaluate the proposed ANFIS-based IDS. We first discuss the experimental setup, including the dataset and evaluation metrics. Then we compare the performance of the proposed IDS with conventional classification models. Afterward, we contrast the detection capability of the ANFIS-IDS with novelty-based IDS [15] for UAVs. Finally, we validate the lightweight nature of the proposed IDS by deploying it on a microcontroller, emulating the hardware of a resource-constrained small UAV.

A. Experimental Setup

This section describes the methodology we employed to evaluate the proposed IDS. To ensure a sound performance validation, we used a consistent data set (referred in Section V) across all the models discussed in the following subsections. Fig. 7 provides an overview of the experimental methodology.

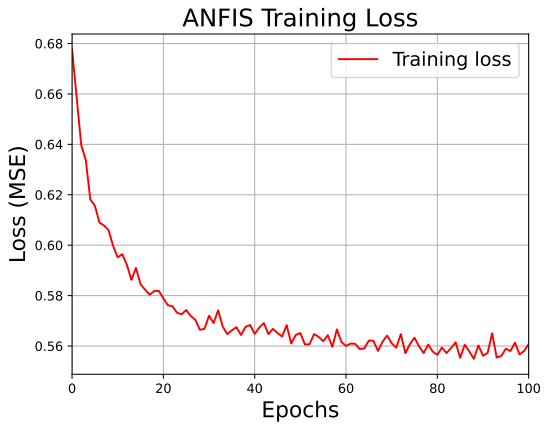
1) Data Split and Training: The data was split into two sets: training and testing. The training set consisted of approximately 16.5k data samples, while the testing set included over 8k data samples. We trained the model for 100 iterations, and the training loss for each iteration is illustrated in Fig. 8(a). We observe that the training loss converges after approximately 60th iteration. Following the completion of training, we evaluated the prediction accuracy of the trained IDS with the test data. Fig. 8(b) presents the overall testing prediction performance via a confusion matrix. It is evident from the confusion matrix is that false negative rate is low, i.e., the proportion of labeling a attack sample as a benign sample is little. Conversely, false positive rate is relatively higher, which is acceptable, since it will not cause any havoc from the security perspective. A more detailed analysis of the performance is provided in the subsequent sections.

2) Evaluation Metrics: We evaluate the performance of the proposed ANFIS-IDS in terms of the following classification metrics:

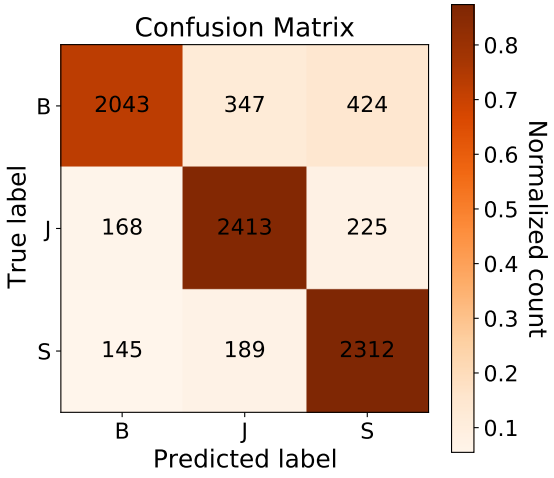
Accuracy: It is a measure that indicates how well a model predicts the correct class or label for a given set of observations. It is calculated by dividing the number of correctly

TABLE II
PERFORMANCE COMPARISON OF CONVENTIONAL CLASSIFICATION MODELS WITH PROPOSED ANFIS-IDS.

Model	Label	Accuracy	Precision	Recall	Specificity	F1 Score
Decision Tree Classifier	*Benign*	0.75	0.857143	0.75	0.924242	0.80021
	GPS Jamming	0.777778	0.777778	0.777778	0.885714	0.777778
	GPS Spoofing	0.833333	0.714286	0.833333	0.868421	0.769231
Gaussian NB	*Benign*	0.60031	0.80021	0.60042	0.909091	0.685714
	GPS Jamming	0.777778	0.875	0.777778	0.942857	0.823529
	GPS Spoofing	0.866667	0.590909	0.866667	0.763158	0.702703
Logistic Regression	*Benign*	0.625	0.806452	0.625	0.888889	0.704225
	GPS Jamming	0.666667	0.705882	0.666667	0.827586	0.685714
	GPS Spoofing	0.666667	0.413793	0.666667	0.776316	0.510638
Linear Discriminant Analysis	*Benign*	0.675	0.818182	0.675	0.90625	0.739726
	GPS Jamming	0.722222	0.722222	0.722222	0.852941	0.722222
	GPS Spoofing	0.785714	0.628571	0.785714	0.828947	0.698413
SVC	*Benign*	0.65	0.8125	0.65	0.903226	0.722222
	GPS Jamming	0.666667	0.666667	0.666667	0.818182	0.666667
	GPS Spoofing	0.846154	0.647059	0.846154	0.842105	0.733333
TSK (ANFIS-IDS)	*Benign*	0.735	0.830508	0.735	0.925	0.779841
	GPS Jamming	0.85	0.858586	0.85	0.93	0.854271
	GPS Spoofing	0.875	0.777778	0.875	0.875	0.823529



(a)



(b)

Fig. 8. Training and testing of proposed ANFIS-IDS: (a) Training loss, and (b) Confusion matrix of testing patterns.

predicted observations by the total number of observations in the dataset.

Precision: It is a performance metric that measures the accuracy of positive predictions made by a model. It calculates the ratio of true positive predictions to the total predicted positive instances, including both true positives and false positives. A higher precision value indicates fewer false positive errors and a greater reliability in identifying positive instances correctly.

Recall: It is a performance metric that measures the ability of a model to identify positive instances correctly. It calculates the ratio of true positive predictions to the total actual positive instances. A higher recall value indicates a lower rate of false negatives and a better ability to capture positive instances accurately.

Specificity: It is a performance metric that measures the ability of a model to correctly identify negative instances. It calculates the ratio of true negative predictions to the total actual negative instances. A higher specificity value indicates a lower rate of false positives and a better ability to accurately identify negative instances. Specificity is used particularly in situations where correctly identifying negative instances is crucial.

F-1 Score: It combines precision and recall into a single measure to provide an overall evaluation of a model's performance. The F1 score is calculated as the harmonic mean of precision and recall. A higher F1 score indicates a better balance between precision and recall, making it a valuable metric for assessing classification models, especially in situations where there is an imbalance between positive and negative classes in the dataset.

ROC curve: Receiver operating characteristic (ROC) curve shows how well a binary classification model performs by comparing its true positive rate to false positive rate at different classification thresholds.

AUC score: Area under the curve (AUC) is a numerical value that summarizes the performance of a binary classification model based on the ROC curve.

B. Validation of ANFIS-IDS performance

This section provides the performance validation of the proposed ANFIS-IDS through, first a comparative analysis

with conventional classification models and then contrasting with a novelty-based IDS.

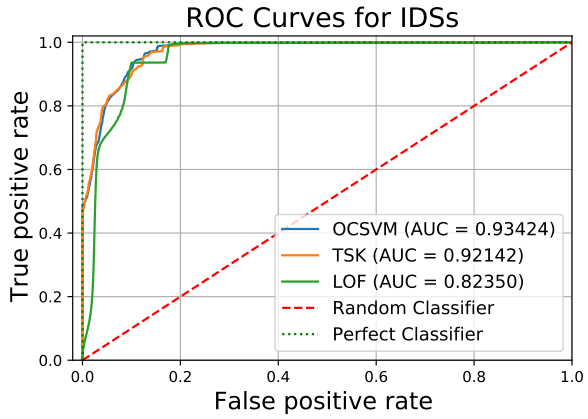


Fig. 9. Comparison with [15] w.r.t. ROC curve and AUC score.

1) Comparison with Classification Models: We perform comparative analysis with the following five conventional classification ML models:

- ***Decision Tree Classifier***: This is a model that uses a tree-like structure to make predictions based on input features. It creates decision rules by recursively splitting the data based on different features to classify new instances. Decision trees are known for their interpretability and effectiveness in classification tasks.
- ***Gaussian Naive Bayes (NB)***: This algorithm is based on Bayes' theorem with the assumption of feature independence. It assumes that the input features follow a Gaussian distribution and uses this information to calculate the likelihood of each class label. The algorithm estimates the probabilities using training data and then classifies new instances based on these probabilities.
- ***Logistic Regression***: It is a binary classification technique that predicts the probability of an instance belonging to a class. It models the relationship between input features and class probabilities using a sigmoid curve. By estimating feature coefficients, logistic regression maximizes the likelihood of observed data. It is widely used, interpretable, and can handle both numerical and categorical features.
- ***Support Vector Classifier (SVC)***: This algorithm finds an optimal hyperplane that maximally separates classes in the feature space. The SVC maps features to a higher-dimensional space and identifies the hyperplane with the largest margin between classes. It assigns class labels based on which side of the hyperplane an input falls. The SVC is effective for complex decision boundaries and can handle high-dimensional data.
- ***Linear Discriminant Analysis***: It is a statistical technique used for dimensionality reduction and classification. It finds a lower-dimensional representation that maximizes class separation by projecting the data onto a linear space. This model assumes Gaussian distribution and similar covariance matrices for the classes. It is effective when classes are well-separated and can be used for feature extraction or direct classification.

TABLE III
COMPARISON WITH IDS IN [15]

IDS	Model	Data	Precision	Recall	F1
Novelty IDS [15]	OCSVM (ν=0.011, γ=2e-4)	*Benign*	1.000	0.704	0.826
		Attack	0.768	1.000	0.868
	LOF (k-neighbours= 3k)	*Benign*	1.000	0.507	0.673
		Attack	0.0526	1.000	0.101
ANFIS-IDS	TSK	*Benign*	1.000	0.735	0.847
		Attack	0.818	1.000	0.899

The results of our performance evaluation, as shown in Table II, highlight some interesting observations. When considering benign signals, the Decision Tree Classifier achieves higher overall metrics, including accuracy and precision, compared to the TSK model of the ANFIS-IDS. However, when evaluating attack signals, the TSK model exhibits significantly higher values in terms of accuracy and recall, surpassing the Decision Tree Classifier. This is of utmost importance since an IDS should be able to detect a majority, if not all, of the true alarms, and a higher recall value indicates a low false negative rate. Although the TSK model shows slightly lower precision in benign data, this is not particularly detrimental for an IDS, as it implies that some benign signals may be falsely classified as attack signals (false alarms), which does not compromise the overall attack detection capability of the IDS. Furthermore, when compared with the other classification models considered, the TSK model consistently achieves higher performance metrics, not only in attack signals but also in benign signals. In terms of both jamming and spoofing attacks, the TSK model outperforms all the machine learning models under consideration. These findings demonstrate the effectiveness and superiority of the TSK model in accurately detecting and mitigating attacks within the UAV network environment.

2) Comparison with Novelty-based IDS: In this section, we delve into a comparative analysis of the proposed ANFIS-IDS with a novelty-based IDS specifically tailored for UAV attack signals. It is important to note that the performance of the ANFIS-IDS in Table III differs from the one presented in Table II since, in this case, we train the TSK model with only two labels by combining jamming and spoofing samples as the attack signals. For the novelty-based IDS, we utilize the One-Class Support Vector Machine (OCSVM) model, setting the hyperparameters ν and γ to 0.0011 and 0.000211, respectively, as suggested in [15]. Additionally, we train the Local Outlier Factor (LOF) model, configuring the hyperparameter k-neighbors to 3000. Upon evaluation, we observe that all models demonstrate flawless performance in detecting the attack signals, achieving perfect recall values. Moreover, the models exhibit perfect precision for benign signals, indicating zero false alarms. To further assess their performance, we compare the ROC curves and AUC scores, as illustrated in Fig. 9. The TSK model employed in the ANFIS-IDS displays a remarkably similar performance to the OCSVM

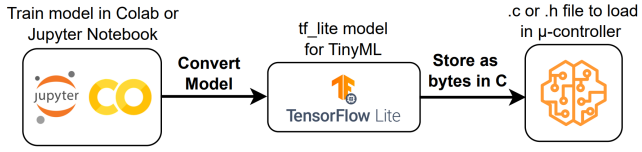


Fig. 10. Deployment of ML models in micro-controllers.

model, while the LOF model exhibits a slightly less steep ROC curve. Evaluating the AUC values, both the TSK model and OCSVM achieve approximately 93% accurate classification, while the LOF model achieves 82% accurate classification. These results highlight the robust performance of the ANFIS-IDS, demonstrating its efficacy in accurately classifying UAV attack signals and achieving comparable performance with state-of-the-art novelty-based IDS models.

C. Evaluation of Lightweight Nature

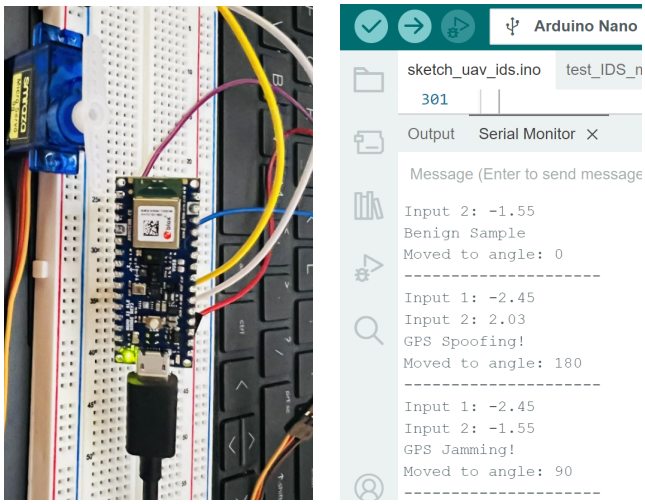
In this section, we evaluate the lightweight nature of the proposed IDS. First, we build a real testbed with a microcontroller, that represents the resource-constrained environment of a small UAV. We deploy two ML-based models (classification and novelty detection) and the proposed ANFIS-IDS model in the testbed to perform comparative analysis. Then we mention some of the μ-controllers with even lesser memory to advocate the usefulness of the proposed IDS.

1) Deploying on μ-controller: Fig. 10 presents the workflow of deploying an ML model in μ-controller, where training is performed in a computational resource-full device, and μ-controller is loaded with the already trained model to act as an interface. First, we trained the ML models in Google Colab [36] and then converted the trained tensorflow models (with final weights and biases) to tensorflowLite models [37] as the TinyML [38]. Finally, we convert the tensorflowLite model to a header file (".h") as byte code, to be loaded to the μ-controller.

TABLE IV
EVALUTION OF LIGHTWEIGHT NATURE

Model	Size (kB)	ExecutionTime (μseconds)
Decision Tree Classifier	25	3845
OCSVM (ν=0.011, γ=2e-4)	20	3958
TSK (ANFIS-IDS)	5	3024

For the ANFIS-IDS, we retrieve the membership functions and rules from the Matlab Fuzzy Logic Toolbox and code the Arduino sketch for the μ-controller. The real testbed implementation is presented in Fig. 11. We utilized Arduino Nano 33 BLE Sense, since it is one of the twelve μ-controllers that are supported by tensorflowLite [39]. We used a servo motor as the actuator device, which will be rotated to different angles according to the detected signal label. For the ANFIS-IDS, we passed the input pattern through the serial monitor, while for the TinyML case, we passed test samples in the sketch. In both cases, the actuation is done at the servo. Table IV presents the evaluation of the ANFIS-IDS's lightweight nature. It is observed that the header files for the ML models are sized four to five times larger than the ANFIS-IDS sketch, meaning ANFIS-IDS will require less space in the SRAM. It



(a) (b)

Fig. 11. Hardware-emulated UAV testbed (resource-limited μ-controller) for deploying IDSs: (a) Arduino Nano 33 BLE with servo as the actuator and (b) Detection results displayed on Arduino IDE serial monitor.

will lead to lower computational requirements, i.e., less power consumption. For untethered edge units like UAVs, it will lead to longer flight times. Again, we compare the execution times required for different models in detecting the label of a given sample. We averaged the execution times from 300 test samples (including 100 samples from each of the three labels) and observed that ANFIS-IDS takes 25% less time than the ML models.

2) Deploying on μ-controllers with lesser memory: Here, we highlight the significance of the proposed IDS by discussing its suitability for μ-controllers with extremely limited flash memory. We consider μ-controllers such as the 'Microchip PIC16F688' and 'STM8S003F3', which possess a mere 8KB of flash memory. Remarkably, this memory capacity is even lower than the sizes of the header files associated with the previously mentioned ML models. This means it is not even possible to load the TinyML models in these low-memory μ-controllers. In this context, the ANFIS-IDS emerges as the exclusive viable choice for such devices with significantly constrained resources.

VII. CONCLUSION

In this work, we design and implement a lightweight IDS based on the ANFIS specifically tailored for resource-constrained small UAV networks. Our IDS demonstrates exceptional capabilities in effectively detecting GPS spoofing and jamming attacks, yielding outstanding performance metrics. To validate the efficacy of our proposed model, we conducted comprehensive evaluations, comparing it against conventional data-driven classification models as well as state-of-the-art IDSs deployed in real-world scenarios. Furthermore, we verified the lightweight nature of our IDS through its successful deployment in a hardware-emulated UAV testbed, which ensured its practical feasibility within resource-limited

environments. To the best of our knowledge, the proposed IDS is the first UAV security solution that leverages ANFIS to specifically address the networking vulnerabilities of these resource-constrained devices, marking a significant milestone in the field. As part of our future work, we will focus on working with a more sophisticated dataset, encompassing diverse attack scenarios and network conditions, to further optimize the ANFIS model and enhance its overall performance.

REFERENCES

[1] H. Shakhatreh, A. H. Sawalmeh, A. Al-Fuqaha, Z. Dou, E. Almaita, I. Khalil, N. S. Othman, A. Khreishah, and M. Guizani, "Unmanned aerial vehicles (uavs): A survey on civil applications and key research challenges," *Ieee Access*, vol. 7, pp. 48 572–48 634, 2019.

[2] A. A. Khalil, M. Y. Selim, and M. A. Rahman, "Cure: Enabling rf energy harvesting using cell-free massive mimo uavs assisted by ris," in *2021 IEEE 46th Conference on Local Computer Networks (LCN)*. IEEE, 2021, pp. 533–540.

[3] B. Fan, Y. Li, R. Zhang, and Q. Fu, "Review on the technological development and application of uav systems," *Chinese Journal of Electronics*, vol. 29, no. 2, pp. 199–207, 2020.

[4] A. A. Khalil and M. A. Rahman, "Fed-up: Federated deep reinforcement learning-based uav path planning against hostile defense system," in *2022 18th International Conference on Network and Service Management (CNSM)*. IEEE, 2022, pp. 268–274.

[5] A. A. Khalil, A. J. Byrne, M. A. Rahman, and M. H. Manshaei, "Replanner: Efficient uav trajectory-planning using economic reinforcement learning," in *2021 IEEE International Conference on Smart Computing (SMARTCOMP)*. IEEE, 2021, pp. 153–160.

[6] A. Jakaria, M. A. Rahman, M. Asif, A. A. Khalil, H. A. Kholidy, M. Anderson, and S. Drager, "Trajectory synthesis for a uav swarm based on resilient data collection objectives," *IEEE Transactions on Network and Service Management*, vol. 20, no. 1, pp. 138–151, 2022.

[7] A. A. Khalil, M. Y. Selim, and M. A. Rahman, "Deep learning-based energy harvesting with intelligent deployment of ris-assisted uav-cfmmimos," *Computer Networks*, vol. 229, p. 109784, 2023.

[8] O. Bouhamed, O. Bouachir, M. Aloqaily, and I. Al Ridhawi, "Lightweight ids for uav networks: A periodic deep reinforcement learning-based approach," in *2021 IFIP/IEEE International Symposium on Integrated Network Management (IM)*. IEEE, 2021, pp. 1032–1037.

[9] G. Choudhary, V. Sharma, I. You, K. Yim, R. Chen, and J.-H. Cho, "Intrusion detection systems for networked unmanned aerial vehicles: a survey," in *2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC)*.

[10] L. M. Da Silva, I. G. Ferrão, C. Dezan, D. Espes, and K. R. Branco, "Anomaly-based intrusion detection system for in-flight and network security in uav swarm," in *2023 International Conference on Unmanned Aircraft Systems (ICUAS)*. IEEE, 2023, pp. 812–819.

[11] P. Sajith and G. Nagarajan, "Network intrusion detection system using anfis classifier," *Soft Computing*, pp. 1–10, 2022.

[12] S. Rahman, M. Ahmed, and M. S. Kaiser, "Anfis based cyber physical attack detection system," in *2016 IEEE 5th International Conference on Informatics, Electronics and Vision*. IEEE, 2016, pp. 944–948.

[13] A. Albanese, M. Nardello, and D. Brunelli, "Low-power deep learning edge computing platform for resource constrained lightweight compact uavs," *Sustainable Computing: Informatics and Systems*, vol. 34, p. 100725, 2022.

[14] L. Teng, M. Jianfeng, F. Pengbin, M. Yue, M. Xindi, Z. Jiawei, C. Gao, and L. Di, "Lightweight security authentication mechanism towards uav networks," in *2019 International Conference on Networking and Network Applications (NaNA)*. IEEE, 2019, pp. 379–384.

[15] J. Whelan, T. Sangarapillai, O. Minawi, A. Almehmadi, and K. El-Khatib, "Novelty-based intrusion detection of sensor attacks on unmanned aerial vehicles," in *Proceedings of the 16th ACM symposium on QoS and security for wireless and mobile networks*, 2020, pp. 23–28.

[16] H.-J. Liao, C.-H. R. Lin, Y.-C. Lin, and K.-Y. Tung, "Intrusion detection system: A comprehensive review," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 16–24, 2013.

[17] B. Wang, Z. Wang, L. Liu, D. Liu, and X. Peng, "Data-driven anomaly detection for uav sensor data based on deep learning prediction model," in *2019 IEEE Prognostics and System Health Management Conference*. IEEE, 2019, pp. 286–290.

[18] J. K. Samriya, M. Kumar, and R. Tiwari, "Energy-aware aco-dnn optimization model for intrusion detection of unmanned aerial vehicle (uavs)," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–16, 2022.

[19] B. Panja, O. Ogunyanwo, and P. Meharia, "Training of intelligent intrusion detection system using neuro fuzzy," in *15th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)*. IEEE, 2014, pp. 1–6.

[20] Y. P. Bria and B. Majhi, "Design and develop application of fuzzy logic controler to determine disaster status early warning to dam tilong central kupang east nusa tenggra," in *ternational Conference*, 2013, pp. 2–4.

[21] N. Walia, H. Singh, and A. Sharma, "Anfis: Adaptive neuro-fuzzy inference system-a survey," *International Journal of Computer Applications*, vol. 123, no. 13, 2015.

[22] A. Chandrasekhar and K. Raghuveer, "An effective technique for intrusion detection using neuro-fuzzy and radial svm classifier," in *Springer NetCom*, 2013, pp. 499–507.

[23] R. A. R. Ashfaq, Y.-l. He, and D.-g. Chen, "Toward an efficient fuzziness based instance selection methodology for intrusion detection system," *International Journal of Machine Learning and Cybernetics*, vol. 8, no. 6, pp. 1767–1776, 2017.

[24] Y. Lei, J. Liu, and H. Yin, "Intrusion detection techniques based on improved intuitionistic fuzzy neural networks," in *2016 International conference on intelligent networking and collaborative systems (INCoS)*. IEEE, 2016, pp. 518–521.

[25] D. Karaboga and E. Kaya, "An adaptive and hybrid artificial bee colony algorithm (aabc) for anfis training," *Applied Soft Computing*, vol. 49, pp. 423–436, 2016.

[26] P. Ganeshkumar and N. Pandeeswari, "Adaptive neuro-fuzzy-based anomaly detection system in cloud," *International journal of fuzzy systems*, vol. 18, no. 3, pp. 367–378, 2016.

[27] H. Moudni, M. Er-rouidi, H. Mouncif, and B. El Hadadi, "Black hole attack detection using fuzzy based intrusion detection systems in manet," *Procedia Computer Science*, vol. 151, pp. 1176–1181, 2019.

[28] G. Choudhary, V. Sharma, I. You, K. Yim, I.-R. Chen, and J.-H. Cho, "Intrusion detection systems for networked unmanned aerial vehicles: A survey," in *2018 14th International Wireless Communications Mobile Computing Conference (IWCMC)*, 2018, pp. 560–565.

[29] M. P. Arthur, "Detecting signal spoofing and jamming attacks in uav networks using a lightweight ids," in *2019 International Conference on Computer, Information and Telecommunication Systems (CITS)*, 2019, pp. 1–5.

[30] O. Bouhamed, O. Bouachir, M. Aloqaily, and I. A. Ridhawi, "Lightweight ids for uav networks: A periodic deep reinforcement learning-based approach," in *2021 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, 2021, pp. 1032–1037.

[31] H. Abdi and L. J. Williams, "Principal component analysis," *Wiley interdisciplinary reviews: computational statistics*, vol. 2, no. 4, pp. 433–459, 2010.

[32] G. Wang, J. Hao, J. Ma, and L. Huang, "A new approach to intrusion detection using artificial neural networks and fuzzy clustering," *Expert systems with applications*, vol. 37, no. 9, pp. 6225–6232, 2010.

[33] R. Sharma, V. A. Athavale, and S. Mittal, "Whale neuro-fuzzy system for intrusion detection in wireless sensor network," in *Advances in Computational Intelligence and Communication Technology: Proceedings of CICT 2019*. Springer, 2021, pp. 123–135.

[34] M. Masdari and H. Khezri, "Towards fuzzy anomaly detection-based security: a comprehensive review," *Fuzzy Optimization and Decision Making*, vol. 20, pp. 1–49, 2021.

[35] J. Whelan, T. Sangarapillai, O. Minawi, A. Almehmadi, and K. El-Khatib, "Uav attack dataset," 2020. [Online]. Available: https://dx.doi.org/10.21227/00dg-0d12

[36] "Google colab," https://colab.research.google.com/.

[37] "Tensorflow lite," https://www.tensorflow.org/lite.

[38] P. P. Ray, "A review on tinyml: State-of-the-art and prospects," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 4, pp. 1595–1623, 2022.

[39] "Tensorflow lite for microcontrollers," https://www.tensorflow.org/lite/microcontrollers.