A Comparative Analysis of Supervised and Unsupervised Models for Detecting GPS Spoofing Attack on UAVs

T. Talaei Khoei[1], A. Gasimova[1], M. A. Ahajjam[1], K. Al Shamaileh[2], V. Devabhaktuni[3], and N. Kaabouch[1]

[1]School of Electrical Engineering and Computer Science, University of North Dakota, Grand Forks 58202, ND, USA
[2]Electrical and Computer Engineering Department, Purdue University Northwest, Hammond 46323, IN, USA
[3]Electrical and Computer Engineering Department, The University of Maine, Orono 04469, ME, USA

2022 IEEE International Conference on Electro Information Technology (eIT) | 978-1-6654-8009-3/22/$31.00 ©2022 IEEE | DOI: 10.1109/eIT53891.2022.9813826

***Abstract*—With the increasing use of Unmanned Aerial Vehicles in military and civilian applications, the security of this technology has become one of the critical concerns. UAVs' positioning and navigation activities are highly dependent on Global Positioning Systems as they provide accurate locations for these vehicles. However, due to the civilian GPS signals being open and unencrypted, malicious users can target them in multiple ways, including by launching Global Positioning System spoofing attacks. To address this security issue, numerous techniques have been proposed to detect and classify these attacks,including supervised machine learning techniques. However, no studies have focused on unsupervised models to detect these attacks. In this paper, we compare the performance of several supervised models with that of unsupervised models in terms of accuracy, probability of detection, probability of misdetection, probability of false alarm, processing time, training time, prediction time, and memory size. The supervised models are Gaussian Naïve Bayes, Classification and Regression Decision Tree, Logistic Regression, Random Forest, Linear-Support Vector Machine, and Artificial Neural Network. The unsupervised models are Principal Component Analysis, K-means clustering, and Autoencoder. The results show that the Classification and Regression Decision Tree model outperforms the other supervised and unsupervised models in detecting and classifying GPS spoofing attacks.**

***Keywords*—classification, comparative analysis, cyber-security, cyber-attacks, clustering, GPS spoofing attacks, machine learning, neural network, spoofing detection, UAVs.**

I. Introduction

The development of unmanned aerial vehicles (UAVs) technology has exploded in recent decades as it has proven to be a valuable tool for many military and civilian applications [1]. Autonomous UAVs usually depend on Global Position Systems (GPS) signals for positioning and navigation. Despite these benefits, this technology is prone to several cyber-attacks [2].

Cyber-attacks on UAVs can be classified as one of three categories: data interception, data manipulation, and denial of service (DoS) [3]. During data interception attacks, data are intercepted during transmission to gain unauthorized access to private information. DoS attacks aim to prevent entities from establishing connections. Data manipulation, on the other hand, involves gaining access to data and altering their content. GPS spoofing attacks are considered one of the most critical attacks on UAVs that fall under this last category. An attacker implementing GPS spoofing sends fake information either by generating new signals or by altering legitimately received signals, leading to an inaccurate display of GPS positions of the targeted device [4].

Several techniques have been proposed to detect and classify GPS spoofing attacks on UAVs. These detection techniques can be divided into three categories, namely, UAV characteristic-based, signal processing-based, and Artificial Intelligence-based. For instance, the authors in [5] proposed a detection technique based on UAV characteristics. They employed a real-time tracking model in order to determine the location of the UAV system. Particularly, a positioning method based on the time difference can locate the position of the UAV formation members within a reasonable error range. Consequently, a malicious attack on a UAV can be identified. This technique was able to detect the attacks with a high accuracy rate. In [6], the authors proposed a signal processing-based method that relies on the UAV onboard camera, as its performance is not affected by the data manipulation attacks. This technique is studied under four UAV Spoofing scenarios using two flight trajectories and two comparison approaches. The first trajectory is obtained from GPS positions, while the second from UAV images using vision odometry. Their proposed approaches consist of two main techniques, direct sum of Euclidian distances and indirect angle distance and taxicab distance between trajectory descriptors.

In addition to these methods, numerous studies have proposed Artificial Intelligence-based techniques, including machine learning (ML) approaches. These approaches are usually classified into two supervised and unsupervised learning techniques. The majority of studies focused on using supervised techniques in addressing this problem. For instance, the authors of [7] compared the performance of four

978-1-6654-8009-3/22/$31.00 ©2022 IEEE

supervised tree-based ML models, namely, Random Forest (RF), Gradient Boosting, extreme Gradient Boosting, and Light Gradient Boosted Machine. The models were evaluated using the probability of detection, probability of misdetection, probability of false alarm, accuracy, processing time, and memory size. Results show the superiority of the extreme Gradient Boosting classifier in detecting GPS spoofing attacks. In [8], the authors proposed a supervised ML model based on an Artificial Neural Network (ANN) and studied its efficiency using different hidden layers and neurons. The top performing networks are the one hidden-layer network with 10 neurons and a two hidden-layers network with six neurons. In [9], two supervised dynamic selection techniques were proposed: Metric Optimized Dynamic selector and Weighted Metric Optimized Dynamic selector. Both approaches dynamically chose the best classifier from 10 supervised conventional ML models. The authors assessed the efficiency of their proposed approach in terms of accuracy, probability of detection, probability of misdetection, probability of false alarm, and processing time.

In [10], the authors proposed a supervised ML-based approach called K-learning. The final result is selected using voting techniques based on accuracy and detection time. In [11], the authors proposed a correlation-based supervised ML model where a Support Vector Machine (SVM) classifier is used along with a correlation analysis to detect signal manipulation attempts on the Global Navigation Satellite System. This method has acceptable results in terms of accuracy.

Nevertheless, a number of limitations can be identified from the literature. The detection of GPS spoofing attacks on UAVs has been formulated as a supervised problem across a wide range of research studies. In such studies, the proposed supervised technique is usually compared with a few conventional supervised models. To the best of our knowledge, there is no study that investigated the performance of unsupervised models in detecting such attacks on UAVs.

Motivated by this research gap, this study provides a comparative analysis of multiple techniques from supervised, and unsupervised models to detect GPS spoofing attacks. We selected five commonly known supervised models, Gaussian Naïve Bayes, Classification and Regression Decision Tree, Logistic Regression (LR), RF, Linear-SVM (L-SVM), and ANN. Unsupervised models include Principal Component Analysis, K-means, and Autoencoder. A dataset with 13 features [7] is used to train, test, and validate the results. Model performance is evaluated in terms of eight metrics: accuracy, probability of detection, probability of misdetection, probability of false alarm, processing time, training time, prediction time, and memory size. To summarize, the contributions of this paper are as follows:

- A comprehensive analysis of the most known unsupervised learning models in terms of selected metrics.
- A performance comparison of multiple unsupervised and supervised learning techniques in terms of multiple evaluation metrics.

The remainder of this paper is as follows: Section II presents the data and techniques employed to develop GPS spoofing attack detection models. Section III reports the experiments and results discussion. The conclusion and future works are provided in Section IV.

II. Materials and methods

In this section, we briefly present the process and all components used to detect GPS spoofing attacks including the considered dataset and the ML models.

A. Model Learning Process and Dataset

The model learning process followed in this work is shown in Fig.1. It consists of several steps: dataset building, data preprocessing, model learning, and performance evaluation. First, real GPS signals are collected and spoofed signals are simulated as described in [7, 12].

Specifically, real GPS signals are collected using software defined radio units and spoofed signals are simulated using MATLAB. Three variations of GPS spoofing attacks are simulated, namely, simplistic, intermediate, and sophisticated attacks. The ensuing signals are processed to extract the set of features used in this work (refer to Table I for the complete list of features). The final dataset consists of 15,000 samples equally distributed between the authentic and spoofed classes. This dataset is preprocessed using two techniques, data imputation and data conversion. More precisely, any null or missing values are discarded from the dataset and a normalization technique, power transformation-based on Yeo-Johnson transformer [13], is used. This technique can transform the numerical input or output to one with a Gaussian-like probability distribution.

TABLE I: List of extracted features.

Extracted features	**Abbreviations**
Carrier to Noise Ratio	C/N0
Magnitude of the Early Correlator	EC
Magnitude of the Late Correlator	LC
Magnitude of the Prompt Correlator	PC
Prompt in-phase correlator	PIP
Prompt Quadrature component	PQP
Carrier Doppler in Tracking loop	TCD
Carrier Doppler	DO
Pseudo-range	PD
Receiver Time	RX
Time of the week	TOW
Carrier Phase Cycles	CP
Satellite vehicle number	PRN

B. Machine Learning Models

Several supervised and unsupervised models are investigated in this study. Although both learning approaches help discover hidden patterns in datasets, supervised techniques require labeled data that can be challenging to collect but can achieve high accuracy. In contrast, unsupervised learning

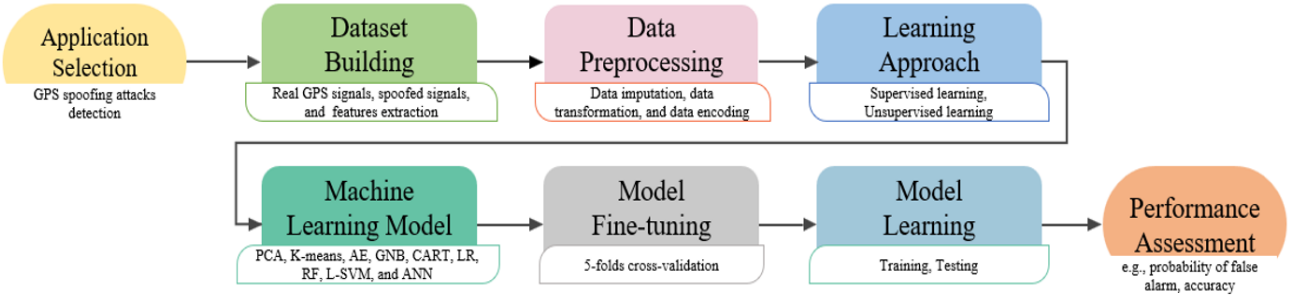

Fig. 1: Model learning process for GPS spoofing attacks detection.

models rely on unlabeled data but generally provide lower accuracy. In addition, such models are more suitable for data analysis tasks as they can identify similarities and differences in the data [14]. Fig.2 provides a classification of the considered learning approaches and their corresponding ML models.

As one can observe, supervised learning models are categorized into six different categories, namely, Bayesian, Tree, Instance, Regularization, Neural Network, and Ensemble-based techniques. From the Bayesian-based category, Gaussian Naïve Bayes (GNB) is selected, which is a type of Naïve Bayes model that supports continuous data. This model is suitable for data with a Gaussian normal distribution. The Classification and Regression Tree (CART) is selected within the Tree-based category. It is a popular model that can take both numerical and categorical variables as inputs. This model uses the Gini index as a splitting criterion and cost-complexity pruning to improve the accuracy and reduce overfitting. Instance-based models category comprises the L-SVM model which can achieve a high accuracy while preventing overfitting. In addition, it is a faster variation of SVMs that employs a linear kernel by default.

In regularization-based models, Logistic Regression (LR) is used, which can model the probabilities for classification problems with binary outputs. It is an extension of the linear regression model that is used for classification rather than regression problems. Artificial Neural Network (ANN) is a type of supervised neural network-based models that consists of three layers, an input, a hidden, and an output layer. It uses an activation function and a learning approach, backpropagation, for the training process. Backpropagation function can measure the gradient of the loss function, with respect of each node weight. The last category of supervised models is known as ensemble techniques. Random Forest is a common type of this category, as it is composed of multiple decision trees, appropriate for classification and regression problems. The prediction result of this model is defined as the class with the majority votes for classification problems and the average vote for regression problems.

Unsupervised learning models are classified into three categories, clustering, Dimensionality Reduction, and Neural

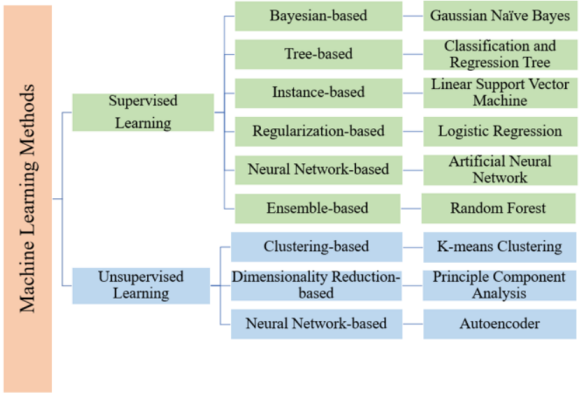

Fig. 2: Classification of model learning approaches and models used in this study.

Network-based techniques, as illustrated in Fig.2. K-means is a common clustering model that is capable of clustering the data by separating them into n groups of equal variances. This process may lead to minimize a criterion, which is known as inertia. Principal Component Analysis (PCA) is a dimensional reduction model that can be used to efficiently reduce the dimensionality of data in a supervised or unsupervised manner. Lastly, Autoencoder is an unsupervised neural network that is widely used to learn a compressed representation of raw data. It consists of an encoder, a latent space representation, and a decoder. The encoder compresses the input data, while the decoder decompresses the encoder's output. After the training process, the encoder is saved, and the decoder can be discarded. The latent space representation holds the necessary data required to represent the original data.

C. Optimization Techniques

Optimization techniques are important to improve the efficiency of ML model and reduce their cost. In this study, an optimization technique that is compatible with the characteristics of all the models is required. For this purpose, grid search optimization is used. This technique is one of the conventional methods for hyperparameter optimization that can perform well on all ML models, excluding neural network techniques. Grid search typically divides the domain of hyperparameters

into a discrete grid. All the combinations in the grid are investigated and evaluated with a cross-validation scheme. The combination that results in the maximum average score is the optimal one.

For neural network-based models, namely, ANN and Autoencoder, a popular method called Adadelta is used [15]. This method is a robust extension of the Gradient Descent Optimization algorithm. It accelerates the hyperparameter tuning process without manual intervention. Table II gives the optimized hyperparameters that have been used in the development of the ML models. Having outlined all stages of the development of the detection model for GPS spoofing attacks, we now proceed to present and discuss the results of our study.

III. Results

In this work, we perform a comparative analysis of nine ML models. A 5- fold cross-validation scheme is used to train 80% of the data and test the remaining 20%. We evaluate the performance of the considered models using eight metrics. The first four metrics (i.e., accuracy, probability of detection P_d, the probability of misdetection P_{md}, and the probability of false alarm P_{fa}) are computed using the following equations:

$$Accuracy = \frac{(T_P + T_N)}{(T_P + T_N + F_P + F_N)} \tag{1}$$

$$P_d = \frac{T_P}{(T_P + F_N)} \tag{2}$$

$$P_{md} = \frac{F_N}{(T_P + F_N)} \tag{3}$$

$$P_{fa} = \frac{F_P}{(T_N + F_P)} \tag{4}$$

where T_P and T_N are the numbers of correctly predicted authentic and spoofed signals, while F_P and F_N are the numbers of incorrectly predicted authentic and spoofed signals. In addition, the following metrics are used:

- Processing time: It defines the amount of time a model spends in the training and testing phases.
- Training time: It defines the amount of time a model spends in the training phase.
- Prediction time: It defines the amount of time a model spends to predict a GPS spoofing attack sample.

Table II gives the optimized hyperparameters used in the development of the ML models, while Fig.3 reports their performances in terms of the first four metrics.

Among the unsupervised models, the Autoencoder model has the best performance. This model has an accuracy of 99.53%, a probability of detection of 99.73%, a probability of misdetection of 0.8%, and a probability of false alarm of 1%. In the contrary the K-means model provides the worst results with an accuracy of 86.23%, a probability of detection of 88.1%, a probability of misdetection of 14.23%, and a probability of false alarm of 8.1%. The PCA model provides acceptable results with an accuracy of 96.34%, a probability of detection of 98.85%, a probability of misdetection of 1.49%, and a probability of false alarm of 1.39%.

Among the unsupervised models, the Autoencoder model achieves the best performance, with an accuracy of 99.53%, a probability of detection of 99.73%, a probability of misdetection of 0.8%, and a probability of false alarm of 1%. The PCA model provides acceptable results with an accuracy of 96.34%, a probability of detection of 98.85%, a probability of misdetection of 1.49%, and a probability of false alarm of 1.39%. In the contrary, the K-means model yields the worst results with an accuracy of 86.23%, a probability of detection of 88.1%, a probability of misdetection of 14.23%, and a probability of false alarm of 8.1%.

The Model performance is further investigated using the other four metrics (refer to Table III). As it can be seen, the Autoencoder model offers the best performances compared with models from its category. It achieves a processing time of 1.69 seconds, a training time of 1.3 seconds, a prediction time of 0.39 seconds, and a memory size of 150.2 MiB. In the contrary, the PCA model has the worst performances with a processing time of 1.876 seconds, a training time of 1.34 seconds, a prediction time of 0.534 seconds, and a memory usage of 170.9 MiB. Among the supervised models, the CART model offers the shortest processing time, training time, prediction time, and the lowest memory usage. While, the ANN model has the worst performances in terms of the

TABLE II: Parameters for models.

Learning approach	Model	Parameters
Unsupervised	K-means	n-clusters = 2, algorithm = 'auto', random-state = 0
	PCA	Criterion = 'entropy', max-depth = 9, Max-features = 'sqrt', splitter = 'best'
	Autoencoder	Loss = 'mse' , Activation = 'Relu', Epoch = 100
Supervised	GNB	var_smoothing = 0.01
	CART	Criterion = 'gini', max-depth = 32, max_features = 'log2', splitter = 'best'
	L-SVM	C = 2, penalty = 'l2'
	LR	Max_iter = 10, penalty = 'l2'
	ANN	Activation = 'identity', alpha = 0.3333, Epoch = 300, solver = 'lbfgs', neurons = 13, hidden layers = 2
	RF	Criterion = 'gini', n_estimators = 5

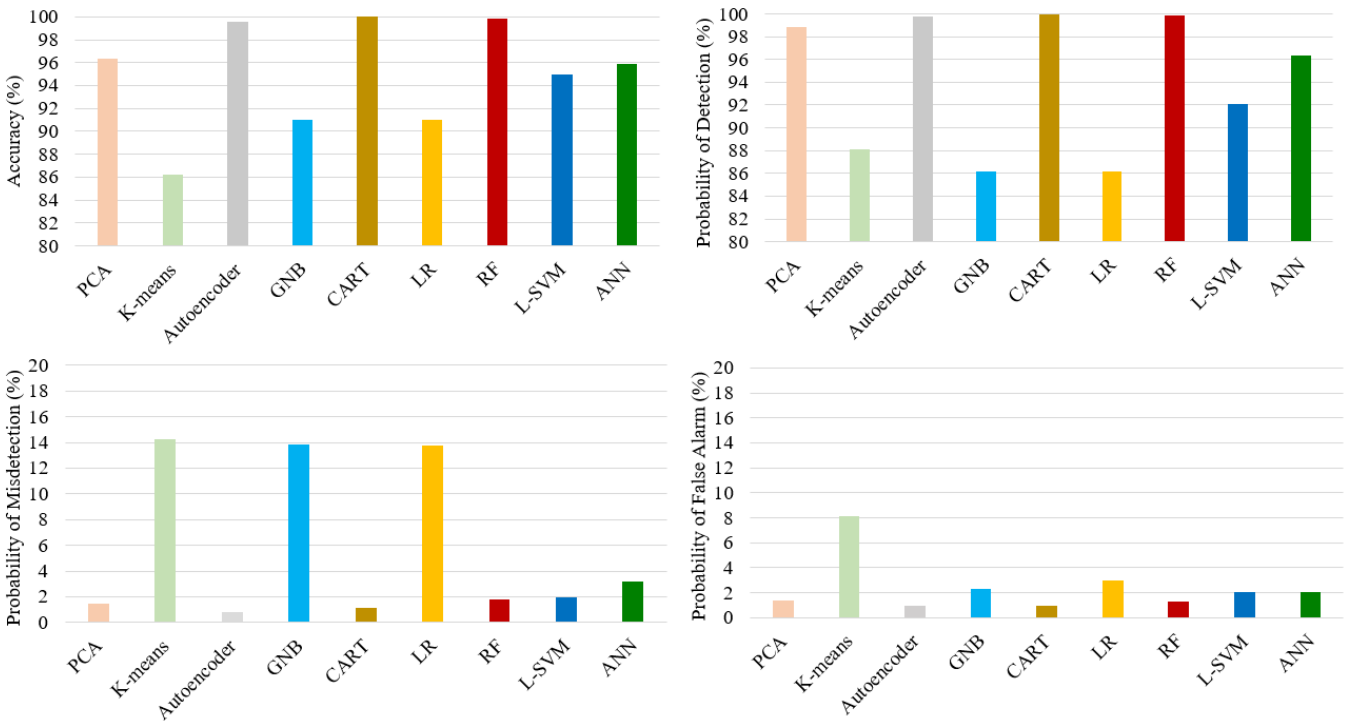

Fig. 3: Performance evaluation of GPS Spoofing attacks detection models in terms of accuracy, probability of detection, probability of misdetection, and probability of false alarm.

TABLE III: PERFORMANCE EVALUATION OF GPS SPOOFING ATTACKS DETECTION MODELS IN TERMS OF PROCESSING TIME, TRAINING TIME, PREDICTION TIME, AND MEMORY SIZE (BEST PERFORMANCES ARE IN BOLD).

Learning Approach	Models	Processing Time	Training Time	Prediction Time	Memory Size
Unsupervised	K-means	1.84s	1.4s	0.4s	166.9MiB
	PCA	1.876s	1.44s	0.437s	170.9MiB
	Autoencoder	**1.69s**	**1.3s**	**0.39s**	**150.2MiB**
Supervised	GNB	4.76s	4.08s	0.68s	250.4MiB
	CART	**1.25s**	**1.14s**	**0.11s**	**142.6MiB**
	L-SVM	3.22s	2.21s	1.01s	280.6MiB
	LR	1.95s	1.33s	0.63s	251.2MiB
	ANN	9.02s	8.09s	0.93s	500.3MiB
	RF	1.7s	1.29s	0.41s	298.4MiB

same metrics. Specifically, the CART model has a processing time of 1.25 seconds, a training time of 1.14 seconds, a prediction time of 0.11 seconds, and a memory usage of 150.2 MiB; and the ANN model has a processing time of 9.2 seconds, a training time of 8.09 seconds, a prediction time of 0.93 seconds, and a memory usage of 500.3 MiB.

It is also apparent that among the unsupervised models, the K-means and the PCA models present relatively close and acceptable performances, while all the other supervised models do not. For instance, the GNB model has a processing time of 4.76 seconds, a training time of 4.08 seconds, a prediction time of 0.68 seconds, and a memory size of 250.4 MiB, which reflect fairly long durations and high memory usage. L-SVM also has a processing time of 3.22 seconds, a training time of 2.21 seconds, a prediction time of 1.01 seconds, and a memory size of 280.6 MiB, showing low performances in terms of these four metrics. To conclude, the main key points of this study are as the following:

- Among supervised and unsupervised learning techniques, the CART model provides the best results in terms of all the considered metrics.
- The GNB model provides the worst results in terms of accuracy, probability of detection, probability of misdetection, probability of false alarm among supervised models, while the ANN model shows long processing time, training time, prediction time, and high memory usage with good accuracy, probability of detection, probability of misdetection, and probability of false alarm.
- Among unsupervised models, the Autoencoder model shows the best performance, while the K-means model

presents the lowest performance in terms of all metrics
- The other models, such as PCA and RF, provide accepted results.

IV. Conclusion

GPS spoofing attacks are one of the most important threats to UAVs. This paper presents a performance analysis of supervised and unsupervised ML models for the detection of GPS spoofing attacks on UAVs. For this purpose, we selected the most known models from each category of supervised and unsupervised learning categories. The unsupervised models are Principal Component Analysis, K-means clustering, and Autoencoder. The supervised models are Gaussian Naïve Bayes, Classification and Regression Decision Tree, Logistic Regression, Random Forest, Linear-Support Vector Machine, and Artificial Neural Network. The performance of every model was assessed in terms of accuracy, probability of detection, probability of misdetection, probability of false alarm, processing time, training time, prediction time, and memory size.The results show that the Classification and Regression Decision Tree is the most efficient in detecting GPS spoofing attack, among all considered unsupervised and supervised models. Future work will include extending this study using online supervised and unsupervised machine learning.

Acknowledgement

The authors acknowledge the support of the National Science Foundation (NSF), Award Number 2006674.

References

[1] D. He, S. Chan, and M. Guizani, "Communication security of unmanned aerial vehicles," *IEEE Wireless Communications*, vol. 24, no. 4, pp. 134–139, 2016.

[2] A. Gasimova, T. T. Khoei, and N. Kaabouch, "A comparative analysis of the ensemble models for detecting gps spoofing attacks on uavs," in *2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)*. IEEE, 2022, pp. 0310–0315.

[3] M. R. Manesh and N. Kaabouch, "Cyber-attacks on unmanned aerial system networks: Detection, countermeasure, and future research directions," *Computers & Security*, vol. 85, pp. 386–401, 2019.

[4] D. Mendes, N. Ivaki, and H. Madeira, "Effects of gps spoofing on unmanned aerial vehicles," in *2018 IEEE 23rd Pacific Rim International Symposium on Dependable Computing (PRDC)*. IEEE, 2018, pp. 155–160.

[5] M. Varshosaz, A. Afary, B. Mojaradi, M. Saadatseresht, and E. Ghanbari Parmehr, "Spoofing detection of civilian uavs using visual odometry," *ISPRS International Journal of Geo-Information*, vol. 9, no. 1, p. 6, 2020.

[6] C. Liang, M. Miao, J. Ma, H. Yan, Q. Zhang, X. Li, and T. Li, "Detection of gps spoofing attack on unmanned aerial vehicle system," in *International Conference on Machine Learning for Cyber Security*. Springer, 2019, pp. 123–139.

[7] G. Aissou, H. O. Slimane, S. Benouadah, and N. Kaabouch, "Tree-based supervised machine learning models for detecting gps spoofing attacks on uas," in *2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*. IEEE, 2021, pp. 0649–0653.

[8] M. R. Manesh, J. Kenney, W. C. Hu, V. K. Devabhaktuni, and N. Kaabouch, "Detection of gps spoofing attacks on unmanned aerial systems," in *2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC)*. IEEE, 2019, pp. 1–6.

[9] T. Talaei Khoei, S. Ismail, and N. Kaabouch, "Dynamic selection techniques for detecting gps spoofing attacks on uavs," *Sensors*, vol. 22, no. 2, p. 662, 2022.

[10] A. Shafique, A. Mehmood, and M. Elhadef, "Detecting signal spoofing attack in uavs using machine learning models," *IEEE Access*, vol. 9, pp. 93 803–93 815, 2021.

[11] S. Semanjski, I. Semanjski, W. De Wilde, and A. Muls, "Use of supervised machine learning for gnss signal spoofing detection with validation on real-world meaconing and spoofing data—part i," *Sensors*, vol. 20, no. 4, p. 1171, 2020.

[12] G. Aissou, S. Benouadah, H. El Alami, and N. Kaabouch, "Instance-based supervised machine learning models for detecting gps spoofing attacks on uas," in *2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)*. IEEE, 2022, pp. 0208–0214.

[13] I.-K. Yeo and R. A. Johnson, "A new family of power transformations to improve normality or symmetry," *Biometrika*, vol. 87, no. 4, pp. 954–959, 2000.

[14] O. Obulesu, M. Mahendra, and M. ThrilokReddy, "Machine learning techniques and tools: A survey," in *2018 International Conference on Inventive Research in Computing Applications (ICIRCA)*. IEEE, 2018, pp. 605–611.

[15] J. Bergstra and Y. Bengio, "Random search for hyper-parameter optimization." *Journal of machine learning research*, vol. 13, no. 2, 2012.