applied sciences

MDPI

Article

Artificial Intelligence-Enabled Exploratory Cyber-Physical Safety Analyzer Framework for Civilian Urban Air Mobility

Md. Shirajum Munir [1,*], Sumit Howlader Dipro [2], Kamrul Hasan [3], Tariqul Islam [4] and Sachin Shetty [1]

[1] Virginia Modeling, Analysis, and Simulation Center, Department of Computational Modeling and Simulation Engineering, Old Dominion University, Suffolk, VA 23435, USA
[2] Department of Computer Science and Engineering, Brac University, 66 Mohakhali, Dhaka 1212, Bangladesh
[3] Department of Electrical and Computer Engineering, Tennessee State University, Nashville, TN 37209, USA
[4] School of Information Studies, Syracuse University, Syracuse, NY 13244, USA
* Correspondence: munir@khu.ac.kr

Abstract: Urban air mobility (UAM) has become a potential candidate for civilization for serving smart citizens, such as through delivery, surveillance, and air taxis. However, safety concerns have grown since commercial UAM uses a publicly available communication infrastructure that enhances the risk of jamming and spoofing attacks to steal or crash crafts in UAM. To protect commercial UAM from cyberattacks and theft, this work proposes an artificial intelligence (AI)-enabled exploratory cyber-physical safety analyzer framework. The proposed framework devises supervised learning-based AI schemes such as decision tree, random forests, logistic regression, K-nearest neighbors (KNN), and long short-term memory (LSTM) for predicting and detecting cyber jamming and spoofing attacks. Then, the developed framework analyzes the conditional dependencies based on the Pearson's correlation coefficient among the control messages for finding the cause of potential attacks based on the outcome of the AI algorithm. This work considers the UAM attitude control scenario for determining jam and spoofing attacks as a use case to validate the proposed framework with a state-of-the-art UAV attack dataset. The experiment results show the efficacy of the proposed framework in terms of around 99.9% accuracy for jamming and spoofing detection with a decision tree, random forests, and KNN while efficiently finding the root cause of the attack.

Keywords: urban air mobility (UAM); exploratory cyber-physical safety analyzer; artificial intelligence; jamming; spoofing; attitude control

check for updates

Citation: Munir, M.S.; Dipro, S.H.; Hasan, K.; Islam, T.; Shetty, S. Artificial Intelligence-Enabled Exploratory Cyber-Physical Safety Analyzer Framework for Civilian Urban Air Mobility. *Appl. Sci.* **2023**, *13*, 755. https://doi.org/10.3390/app13020755

Academic Editors: Shanling Dong and Meiqin Liu

Received: 29 November 2022
Revised: 28 December 2022
Accepted: 31 December 2022
Published: 5 January 2023

1. Introduction

In recent years, urban air mobility (UAM) has significantly gained the attention of smart citizens for providing daily life services such as package delivery, surveillance, agriculture monitoring, passenger flying cars, and rescue management. With the increasing usage of civilian UAM, the risk of cyberattack and theft is also growing exponentially due to the utilization of public network infrastructure [1–7]. However, UAM safety can be increased by proactively monitoring UAM behavior from their operational control messages and employing the capability of analyzing such behavior. In particular, the UAM service provider must require an analytical tool that can intuit the cause of safety threats and visualize the difference between normal and abnormal activities from UAM operational messages in real time. One suitable way of developing this is by unitizing the notion of lightweight artificial intelligence (AI) and inferring the outcomes using statistical analysis so that UAM service providers can take necessary safety measures in advance for protecting UAM from cyberattacks, losses, and crashes.

1.1. Motivation and Challenges

Within the scope of this study, our primary focus is on the safety of the UAM attitude control system to guard against both crashes and theft, which are cause by cyberattacks such as jamming and spoofing. Since the majority of research [1–8] on unmanned aerial vehicles (UAVs) has focused on how to exploit vulnerabilities in received signal indicators (RSSIs) or communication streams. Unlike that, our method is new and distinct, since we are not only detecting the cyber threat but also providing analytics on the risk of a cyberattack. In addition, a significant portion of the research literature has focused on the detection of intrusions in aerial vehicles without providing or expanding upon the attack mechanism excluding the attitude control system. One of our main goals is to conduct an extensive experimental study of the exploratory cyber-physical safety framework that incorporates artificial intelligence and statistical models. As a result, our study becomes unique in identifying and validating cyberattacks, following attitude control system protocols while exploring the vulnerabilities of communication streams.

In order to achieve such a goal, we have faced several technical challenges. A few of the technical challenges are summarized as follows:

- First, the prediction of UAM cyberattacks must be taken as a fraction of the time (e.g., 1–10 ms). Then, the question is how we can meet such a requirement while, in general, AI mechanisms are computationally expensive.
- Second, designing a lightweight AI mechanism can be one of the suitable methods, where offline training and online execution can solve such challenges. However, it is hard to detect the root cause of cyberattacks dynamically when a pretrained model is used. Now, the challenge is how to ensure analyticity so that the UAM service providers can autonomously find the risk of theft and crashes.
- Finally, an AI-enabled exploratory cyber-physical safety analyzer framework for civilian UAM operations can overcome the above challenges. However, it is imperative to meet the distinct characteristics of several UAM examples, since the manufacturing and working principles vary among them.

1.2. Contributions

To solve the aforementioned challenges, we summarize the key contributions of this work as follows:

- First, we design an AI-enabled exploratory cyber-physical safety analyzer framework for civilian UAM operations. The proposed framework can predict, analyze, and protect civilian UAM from cyber threats by detecting jamming and spoofing through analyzing the control message and attitude observation.
- Second, we apply AI algorithms such as decision trees [9], random forests [10], logistic regression [11], K-nearest neighbors (KNN) [12], and long short-term memory (LSTM) [13] for predicting and detecting cyber jamming and spoofing attacks for civilian UAM. We analyze the performance of the applied AI algorithms using the state-of-the-art *UAV attack dataset* [14].
- Third, we devise a security analyzer that can determine conditional dependencies by the Pearson's correlation coefficient [15] among the control messages and attacks based on the outcome of the AI algorithm. In particular, the security analyzer can characterize the abnormal behavior of UAM attitude control and radio frequency-based signals to protect commercial UAVs from theft and crashes.
- Finally, we conduct rigorous experimental analysis of the proposed AI-enabled exploratory cyber-physical safety framework. We have found that almost all of the causes of jamming and spoofing attacks can be detected and verified by the proposed system, which can reduce the risk of theft and crashes in commercial UAVs.

The rest of this paper is organized as follows: We discuss some of the interesting related works in Section 2. Section 3 presents the considered system model and problem description. Then, we propose our AI-enabled exploratory cyber-physical safety analyzer framework for civilian UAM operations in Section 4. Detailed experimental analysis and the key findings are given in Section 5. Finally, we conclude our discussion in Section 6.

2. Related Works

In this section, we discuss some of the interesting research that has addressed the cybersecurity of UAVs and their communication networks. In [5], the authors applied machine learning models for vulnerability and cyberattack detection. However, this work does not provide any analytical mechanism that can infer the root cause of such kinds of cyberattacks. A convolutional neural network (CNN)-based UAV attitude estimation mechanism was proposed in [6]. However, the authors did not consider cyberattacks on a UAV's attitude control that are caused by jamming or spoofing. Recently, in [8], the authors provided a gap analysis for the security flow of UAV networks. This work does not provide any technical presentation that can reduce the security gap in UAV communication systems.

The authors in [16] investigated UAV cyberattacks on a very small scale, such as attack vectors, two jamming and four spoofing attacks, and two communication and two data stream assaults. Here, they prioritized GPS jamming and spoofing over communication and data stream attacks. However, this work concentrated on combating GPS jamming and spoofing by overlooking the attacks on data and control systems. In our work, we are conducting research with an emphasis on attacks on the attitude control system by jamming and spoofing. In [7], the authors pointed out the vulnerability of cybersecurity threats in long-range UAVs in dangerous areas. Numerous threats were discussed, including the possibilities of attacks on ground stations, GPS spoofing and jamming, Wi-Fi attacks, poisoning cellular networks with Denial of Service (DoS), jamming and spoofing, and adversarial attacks in UAV communications. However, they did not give any strong solution to saving long-range UAVs from jamming and spoofing. Rather, they focused on examining the details of security analysis in ground stations.

The main aim of the jamming attack is to inhibit communication in the transmission process by interfering with the ability to receive signals [17,18]. Moreover, following a pattern of continuous radio signal transmission, a jamming model randomly switches between those signals so they can form a mimic model, which is a reactive jammer model that can predict the control of a hacker manipulating the trajectory of a UAV by obtaining information on collision avoidance features. In [19], the authors inspected jamming attacks on sensor networks and how to tackle these attacks. The authors of [19] also showed various attack planning that can be harmful to sensor networks, and after that, they presented two strategies for detecting these attacks. However, they completely ignored that possible attacks on UAVs can be against the attitude sensor system or received signal strength indicator which, in our paper, we will address with our framework.

In [20], the authors investigated how a GPS spoofing fault detector can be used in real time to prevent a UAV from being driven to a harmful destination. A simulator, UAVsim, was used for detection of spoofing and jamming attacks in [21]. In our work, we build an analytical framework which can detect an attack on the switching states' received signal strength indicator. The work in [22] presented behavior-rule-based UAV intrusion detection system (IDS) (BRUIDS). In particular, their BRUIDS are capable of detecting intrusions by triggering based on the specifications of the IDS if the UAV is misdirected due to GPS spoofing. Even though these IDSs operate well in attack responses, the boundaries on the control system and the surrounding limits prevent IDS use in UAVs.

In [23], the author proposed a classifier framework for identifying intrusions that can attack UAVs. However, this framework, which they named the one-class classifier, needs flight log data for training that must be non-anomalous. The authors used methods such as an SVM, autoencoder neural network, and local outlier factor classifier. In addition, using these models, they found the autoencoder neural network to be promising for GPS spoofing detection. In [24], GPS spoofing attacks confined by a sequential probability ratio detector were explored. Nevertheless, there was no investigation into guiding the UAV to an arbitrary hostile location. In our cyber-physical safety framework, we elaborate on GPS jamming and spoofing attacks on the civilian UAM attitude control system in such a way that the UAM service provider can predict the risk of jamming and spoofing attacks as well as find the root causes of such attacks. A detailed system model and problem description are given in the following section.

3. System Model and Problem Description

We consider a delivery urban air mobility infrastructure in a wireless network, where RF signals and their sensory observation autonomously control the delivery drones as shown in Figure 1. Jamming and spoofing are the most common attacks for commercial UAM. The attacker attacks to steal the UAV and corresponding delivery goods, while in some cases, the intention is to crash the UAV. We consider that $d \subset \mathcal{D}$ is N-dimensional data that control the UAM attitude and a binary variable $\hat{x} = \{0, 1\}$, where $\hat{x} = 1$ denotes an attack; otherwise, it is 0. Using the observation of historical UAM operational data, we can train the AI model. Consider each historical observation $d \subset \mathcal{D}$ labeled with a binary indicator $x = \{0, 1\}$. Then, we can define the AI model as a function of historical observation $d \subset \mathcal{D}$, given the label $x = \{0, 1\}$. The learning model can defined as follows:

$$f(\mathcal{D}|x) = \min \phi(\sum_{\forall d \in \mathcal{D}} |x - \hat{x}|), \tag{1}$$

where $\hat{x} = 1$ denotes an attack; otherwise, it is 0.

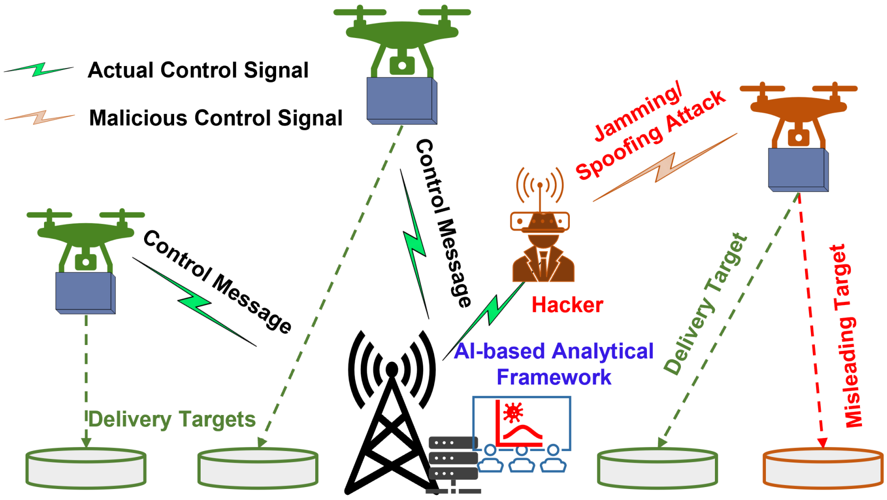

Figure 1. System model of urban air mobility cyber-physical system.

In this work, our goal is to develop an AI-enabled analytical framework to predict and protect UAVs from cyberattacks and crashes. Therefore, we consider the data $\mathcal{D}$ that include the behavior of a UAV's attitude [6,25] and their changes in Equation (1) so that we can proactively detect abnormal attitudes caused by jamming or spoofing attacks. Therefore, it is imperative to build an analytical model based on the outcome of Equation (1) to proactively manage a UAV under a cyber-physical threat. In this work, we consider the Pearson's correlation coefficient [15] to analyze an upcoming event $\hat{x}$. The Pearson's correlation coefficient [15] model for current UAM observation $\hat{d}$ is formalized as follows:

$$g(A, B) = \frac{\mathrm{E}(AB) - \mathrm{E}(A)\mathrm{E}(B)}{\sqrt{\mathrm{E}(A^2) - \mathrm{E}(A)^2}\sqrt{\mathrm{E}(B^2) - \mathrm{E}(B)^2}}, \tag{2}$$

where A and B are two random variables of UAM observation $\hat{d}$. Therefore, the correlation coefficient for N-dimensional UAM in the observation $\hat{d}$ can be represented as follows:

$$G(\hat{d}|\hat{x}) = \sum_{n \in N} \frac{\mathrm{E}(A_n B_n) - \mathrm{E}(A_n)\mathrm{E}(B_n)}{\sqrt{\mathrm{E}(A_n^2) - \mathrm{E}(A_n)^2}\sqrt{\mathrm{E}(B_n^2) - \mathrm{E}(B_n)^2}}. \tag{3}$$

Equation (3) can determine the effect of the decision of the variable $\hat{x} = \{0, 1\}$.

In this system model, our goal is to predict the status of a cyberattack $\hat{x}$ using the trained model in Equation (1) and analyze the effect of that result on a UAM control message, such as longitudinal and roll, transverse and pitch, and vertical and yaw motions for controlling UAM attitude. Furthermore, the Pearson's correlation coefficient-based analytical model can find the switching states and received signal strength indicator of switching states so that the UAV becomes protected from being stolen or lost. In other words, the proposed exploratory cyber-physical safety analyzer framework can proactively detect jamming and spoofing attacks on UAVs while also being capable of analyzing the changes in parameters' values which are caused by such attacks. The UAM hacker or hijacker may set a target to steal or crash a UAV, which ends up as a loss of a UAV for the owner. Based on the proactive detection and characterizing changes of the parameters, the UAM provider can take the necessary steps to protect UAM from theft or loss by updating the UAM controlling parameters.

The proposed system model provides a generic framework, where an AI model $f(\mathcal{D}|x)$ can be trained by using existing AI algorithms that include decision trees, random forests, logistic regression, KNN, and LSTM to detect jamming and spoofing attacks. The analytical model $G(\hat{d}|\hat{x})$ of UAM protection is used with the Pearson's correlation coefficient mechanism to find the relationship between the control messages and abnormal behavior by a UAV. In the following section, we will describe the proposed exploratory cyber-physical safety analyzer framework for commercial UAM.

4. Proposed Exploratory Cyber-Physical Safety Analyzer Framework

The AI-enabled exploratory cyber-physical safety analyzer framework for civilian UAM operations is depicted in Figure 2. In this framework, we devise a modular design by utilizing the concept of an AI pipeline. The proposed framework first analyzes the historical UAM operational data for feature selection, finding a correlation and missing value imputation. For example, if we consider UAM attitude control, then we need to analyze the sensor measurements and their changes, since jamming or spoofing attacks may change the behavior of a UAV's attitude operation. This sensor observation includes longitudinal and roll, transverse and pitch, and vertical and yaw motions to predict the abnormal behavior of a UAV.

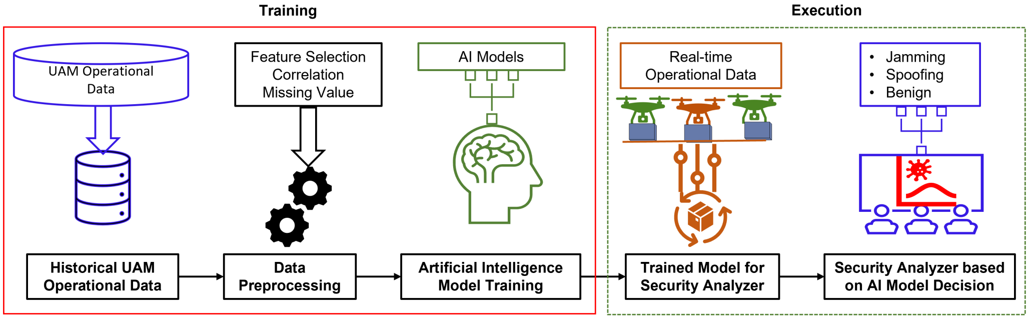
Training
Execution
UAM Operational Data
Feature Selection
Correlation
Missing Value
AI Models
Real-time Operational Data
• Jamming
• Spoofing
• Benign
Historical UAM Operational Data
Data Preprocessing
Artificial Intelligence Model Training
Trained Model for Security Analyzer
Security Analyzer based on AI Model Decision

Figure 2. Modular view of the proposed artificial intelligence-enabled exploratory cyber-physical safety analyzer framework for civilian urban air mobility operations.

In this framework, we can train several AI models based on the requirements of the UAM security analyzer. The AI models are trained based on the principle of existing algorithms in a supervised manner. Thus, in this work, we have developed decision tree [9], random forest [10], logistic regression [11], K-nearest neighbors (KNN) [12], and LSTM [13] schemes on top of the proposed framework for justifying the performance of the proposed cyber-physical safety analyzer framework. Furthermore, the trained models are saved for real-time deployment in a security analyzer to protect commercial UAVs from cyberattacks and theft.

The security analyzer utilizes a training model for ensuring cyber-physical safety for commercial UAM. In particular, based on the analysis of real-time UAM operational data through the trained AI model, the security analyzer can predict and find the cause of security threats by deploying the Pearson's correlation coefficient [15]. The proposed framework is trained offline via historical operational data and executed in real time by using a trained model and current UAM operational data.

The training and execution procedure of the proposed AI-enabled exploratory cyber-physical safety analyzer is given as follows:

- Offline training (red rectangle in Figure 2)
    1. Collect historical UAM operational data;
    2. Preprocessing historical datasets for feature selection and missing value interpretation through averaging;
    3. Deploying AI algorithms such as decision trees [9], random forests [10], logistic regression [11], K-nearest neighbors (KNN) [12], and long short-term memory (LSTM) [13] for security analyzer model training using Equation (1);
    4. Save the trained models.
- Real-time execution and analyzing threats (green-dashed rectangle in Figure 2)
    1. Load the trained model and use real-time UAM operational data for predicting cyber threats such as jamming and spoofing;
    2. Based on the outcome of the AI model, execute the Pearson's correlation coefficient [15] matrix in Equation (3) for analyzing the findings for UAM safety;
    3. Take necessary actions using the findings.

Offline training and real-time execution of the proposed AI-enabled exploratory cyber-physical safety framework were physically deployed in a centered controller of a commercial UAM infrastructure. We developed the proposed exploratory cyber-physical safety framework in the Python platform [26]. A detailed description of the experiment is discussed in the next section.

5. Experimental Analysis

5.1. Experiment Set-Up and Dataset Description

In this work, we used the configuration of a processor consisting of an Intel Core i5-10400 CPU with 16 GB of RAM on a 64 bit operating system. Moreover, we also utilized the Google Colab environment, which gave us an extra 12 GB of RAM for implementation. We used the UAV attack dataset from [14]. The authors of this dataset used the ULOG file format in their research, which was utilized for the saving of flight logs by the autopilot function. Despite the fact that flight logs can have a variety of formats and contain a wide variety of information, standard characteristics are always recorded for post-flight analysis. In our numerical representation, we considered each kind of abnormal behavior, such as jamming and spoofing, which we represented with 1, and normal behaviors were represented by 0. Primarily, we set out to measure the attack segment of our data with the sensor measurements and measurement changes from the dataset through a correlation matrix or linear independence.

In this work, we considered a UAM attitude control scenario to train the AI models for determining jamming or spoofing attacks. Figure 3 shows the working principle of the UAM attitude control mechanism with six degrees of freedom through yaw, pitch, and roll. Therefore, we used UAM attitude data that consisted of timestamped parameters, reference points, roll and longitudinal, transverse and pitch, and vertical and yaw motions, reference change, roll change, pitch change, and yaw change. We considered three distinct data for characterizing jamming ($ace\text{-}jamming\text{-}log$_1_2033-8-19-16-46-46_$vehicle_attitude$_0.$csv$), spoofing ($ace\text{-}spoofing\text{-}hackrf\text{-}log$_5_2033-8-19-17-14-18_$vehicle_attitude$_0.$csv$), and benign attacks ($ace\text{-}benign\text{-}log$_0_2033-8-19-16-27-30_$vehicle_attitude$_0.$csv$) in the considered dataset [14]. Then, we analyzed the impact of the detected cyber threats on the parameters of the switching state (px4io) and radio status of the UAVs by using px4io and radio status data. In particular, we considered *ace-spoofing-hackrf-log*_5_2033-8-19-17-14-18_*px4io*_*status*_0.*csv* and *ace-spoofing-hackrf-log*_5_2033-8-19-17-14-18_*radio*_*status*_0.*csv* for spoofing, *ace-jamming-log*_1_2033-8-19-16-46-46_*px4io*_*status*_0.*csv* and *ace-jamming-log*_1_2033-8-19-16-46-46_*radio*_*status*_0.*csv* for jamming, and *ace-benign-log*_0_2033-8-19-16-27-30_*px4io*_*status*_0.*csv* and *ace-benign-log*_0_2033-8-19-16-27-30_*radio*_*status*_0.*csv* for benign cases. On the one hand, to find the impact of jamming, spoofing, and benign cases on the switching state (PX4IO Status), we considered the servo rail voltage in volts and RSSI pin voltage in volts as parameters. On the other hand, the RSSI, remote RSSI, transmit buffer, noise, and remote noise were considered as the parameters for finding the impact of jamming, spoofing, and benign cases on the radio status of a UAV.

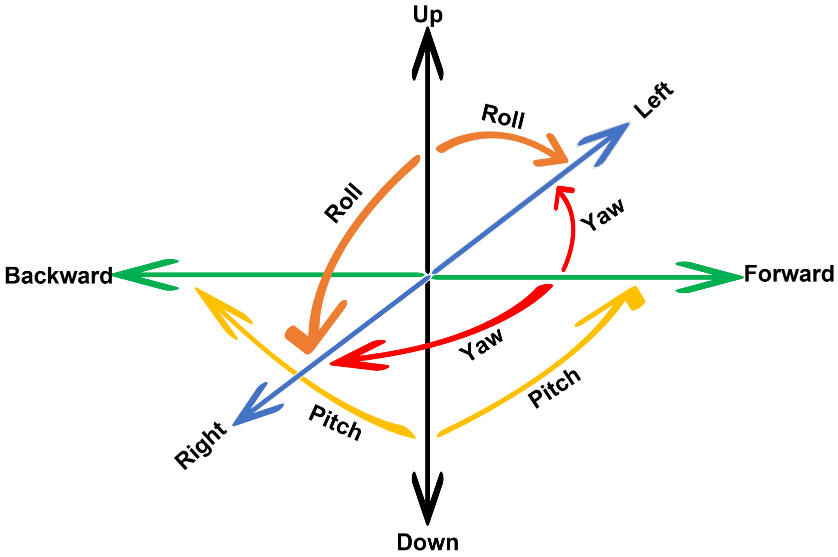

Figure 3. Illustration of six degrees of freedom by yaw, pitch, and roll for UAM attitude control.

We illustrate a correlation matrix between attacks and UAM attitude control parameters in Figure 4. Figure 4 shows a strong correlation among attacks and UAM attitude parameters such as yaw (72%), pitch changes (88%), and yaw changes (88%). Figure 4 also demonstrates a roughly 91% negative correlation between spoofing or jamming attacks and the timestamps. In summary, in Figure 4, we found that the attack data had a strong positive correlation with two measurement changes, which were the transverse and roll changes and the vertical and yaw changes, while the attack data had a strong correlation with one sensor measurement: yaw motion. Furthermore, we show the principal component analysis (PCA) of the considered dataset in Figure 5. Figure 5 also provides evidence of the prominent effects of pitch changes, yaw changes, and roll changes on spoofing or jamming attacks.

Data preparation is a fundamental prerequisite for training a model, as the amount of training data is typically very high. In our case, we considered 7159 sessions as attacks and 4924 sessions as not attacks. Following that, we partitioned the data into two sections: the training section and the testing section. Both of these sections were distinct with attack and not attack portions. We set aside 80% of the data for the training test and 20% for the actual test. Additionally, in this experiment, we utilized the concept of cross-validation using the GridSearchCV API [27]. Therefore, we did not need to allocate dedicated data for the validation, while the training data were automatically split through the API based on cross-validation generator parameters. For instance, we set the cross-validation parameter to be 10 for KNN, which means the training set would be split into 10 partitions, and we would alternatively consider each partition as a validation set.

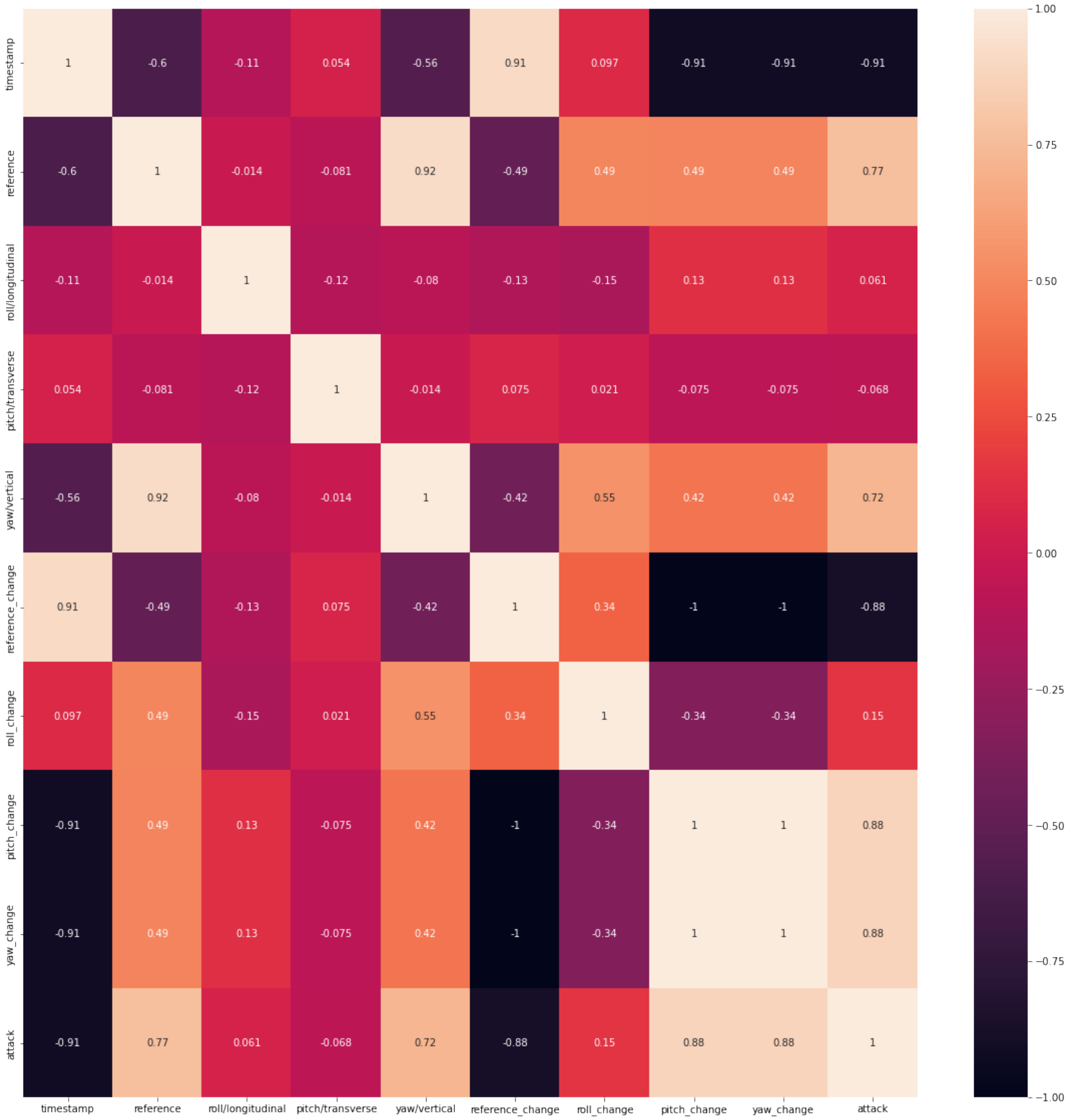

Figure 4. Correlation matrix between attacks (spoofing or jamming) and UAM attitude control parameters.

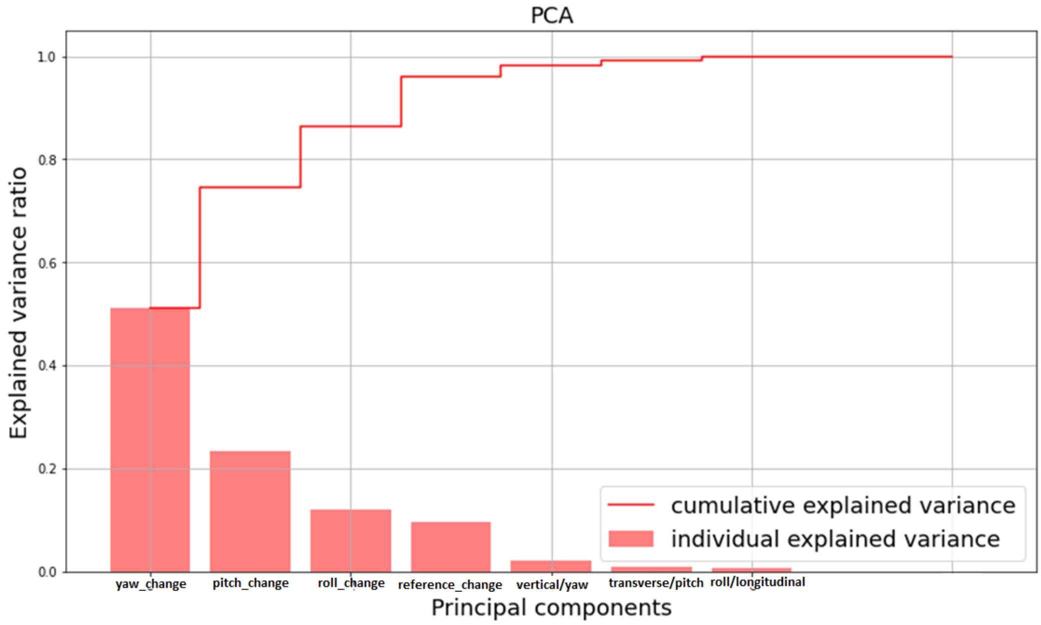

Figure 5. Principal component analysis (PCA) of the considered dataset for detecting attacks (spoofing or jamming) in UAM attitude control.

We have summarized our key parameters in Table 1 so that interested readers can reproduce the results. We considered a k-range from 1 to 100 for checking the neighbors to achieve the best classification. During the KNN training, we chose 10-fold cross-validation for mitigating the bias for determining spoofing or jamming attacks. We also considered the number of neighbors to be 79, while the weights were considered in a uniform distribution. We set 0.8 as an inverse of the regularization strength for the LR, since a smaller value could deal with strong regularization. In the case of random forest classification, we selected the random state to be 42, the number of estimators to be 50, and the maximum depth to be 8. We chose a maximum depth of 5 and minimum sample leaf $(3, 6, 10)$ for grid search-based decision tree training. Furthermore, we performed 10-fold cross-validation during this model training. In the case of LSTM model training, we considered 50 LSTM units, 100 epochs, and a batch size of 155 due to the time dependency among each training data point. We evaluated the mean absolute error (MEA) and executed an ADAM optimizer for LSTM model training.

Table 1. Summary of experiment set-up.

Parameter Name	Value
K-range (KNN)	$(1, 100)$
Cross-validation (KNN)	10
N-neighbors (KNN)	79
C (logistic regression)	0.8
Random state (random forest)	42
Cross-validation (random forest)	5
N-estimators (random forest)	50
Cross-validation (decision tree)	10
LSTM units in cell	50
No. of epochs (LSTM)	100
Batch size (LSTM)	155

5.2. Evaluation Metric and Methodology

We implemented decision trees, random forests, logistic regression, KNN, and LSTM for validating the proposed exploratory cyber-physical safety framework for commercial UAM. Furthermore, we evaluated the algorithms by utilizing confusion matrices that could allow us the measurement of false positive and false negative results [5]. Furthermore, we evaluated the proposed schemes using well-established evaluation metrics such as the precision, recall, F1-score, and accuracy of the AI mechanism. In other words, we fed the data to the KNN, logistic regression model, random forest classifier, decision tree classifier, and LSTM model for predicting the accuracy of attacks from the attacker. We have not provided a detailed working procedure of each AI algorithm, since we used and deployed the Scikit APIs [26] for each ML model. We refer to the following base paper reference for further reading on the decision tree [9], random forest [10], logistic regression [11], KNN [12], and LSTM approaches [13].

We illustrate a block diagram of the overall methodology with the inputs and outputs in Figure 6. We considered UAM attitude control parameters such as the input timestamp, reference point, roll and longitudinal, transverse and pitch, vertical and yaw, reference change, roll change, pitch change, and yaw change inputs as shown in Figure 6. The inputs were prepossessed by missing value interpretation and adding a label of jamming or spoofing and benign. We implemented decision trees [9], random forests [10], logistic regression [11], KNN [12], and LSTM [13] on the Python platform [26,27]. Then, each trained model was tested by the test dataset and used to predict the jamming or spoofing and benign behavior of UAVs. Based on this detection, the proposed framework found the root cause and effect of the servo rail voltage and RSSI pin voltage for the switching state (PX4IO Status) parameters. Furthermore, the proposed framework could also analyze the impact of radio status parameters such as the RSSI, remote RSSI, transmit buffer, noise, and remote noise for finding the impact of jamming or spoofing and benign cases (as shown in Figure 6). Therefore, our cyber-physical safety analyzer could detect all kinds of attacks such as jamming and spoofing from attitude control system and explain the root cause on a radio frequency-based communication signal.

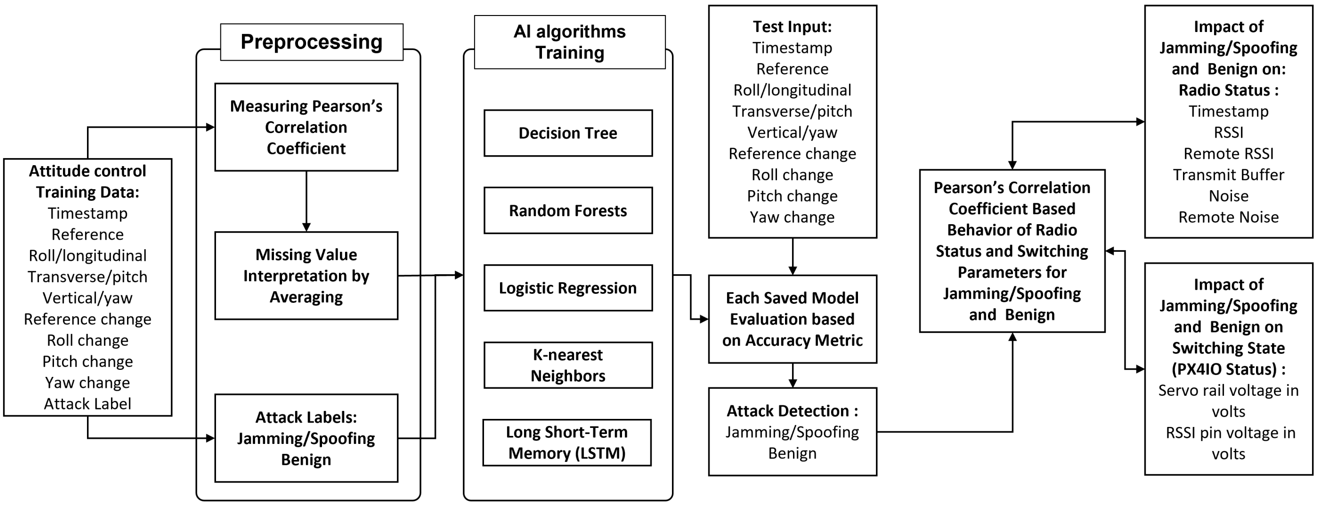
Attitude control Training Data:
Timestamp
Reference
Roll/longitudinal
Transverse/pitch
Vertical/yaw
Reference change
Roll change
Pitch change
Yaw change
Attack Label
Preprocessing
Measuring Pearson's Correlation Coefficient
Missing Value Interpretation by Averaging
Attack Labels: Jamming/Spoofing Benign
AI algorithms Training
Decision Tree
Random Forests
Logistic Regression
K-nearest Neighbors
Long Short-Term Memory (LSTM)
Test Input:
Timestamp
Reference
Roll/longitudinal
Transverse/pitch
Vertical/yaw
Reference change
Roll change
Pitch change
Yaw change
Each Saved Model Evaluation based on Accuracy Metric
Attack Detection : Jamming/Spoofing Benign
Pearson's Correlation Coefficient Based Behavior of Radio Status and Switching Parameters for Jamming/Spoofing and Benign
Impact of Jamming/Spoofing and Benign on: Radio Status :
Timestamp
RSSI
Remote RSSI
Transmit Buffer
Noise
Remote Noise
Impact of Jamming/Spoofing and Benign on Switching State (PX4IO Status) :
Servo rail voltage in volts
RSSI pin voltage in volts

Figure 6. Block diagram of overall methodology with inputs and outputs.

5.3. Results and Discussion

First, we demonstrate the numerical analysis of the longitudinal and roll, transverse and pitch, and vertical and yaw motions on jamming and spoofing attacks in Figures 7–9, respectively. These analyses demonstrate jamming and spoofing attacks on the attitude control message of UAVs becoming more effective during UAV travel.

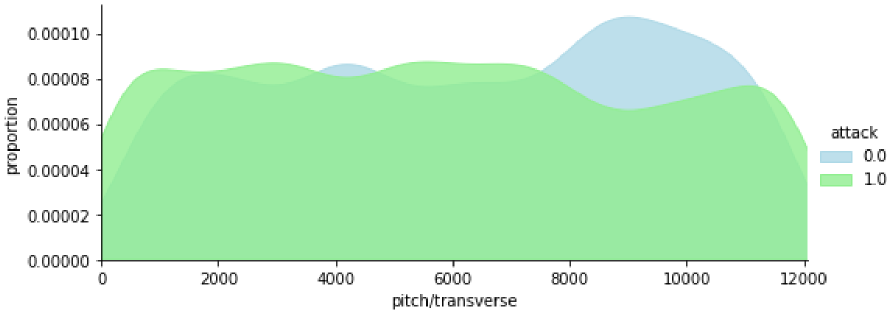

Figure 7. Numerical feature analysis of attacked longitudinal and roll motions.

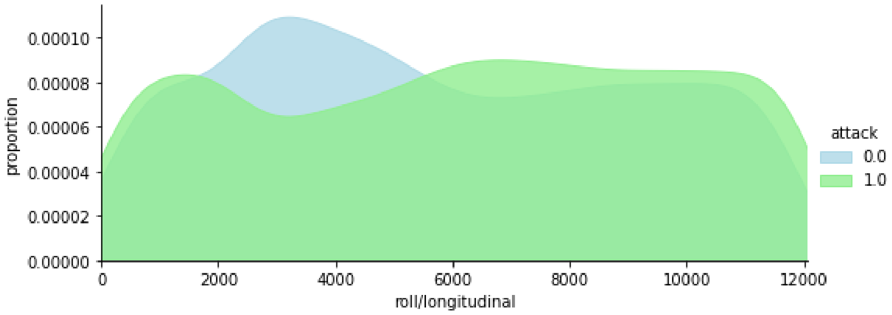

Figure 8. Numerical feature analysis of attacked transverse and pitch motions.

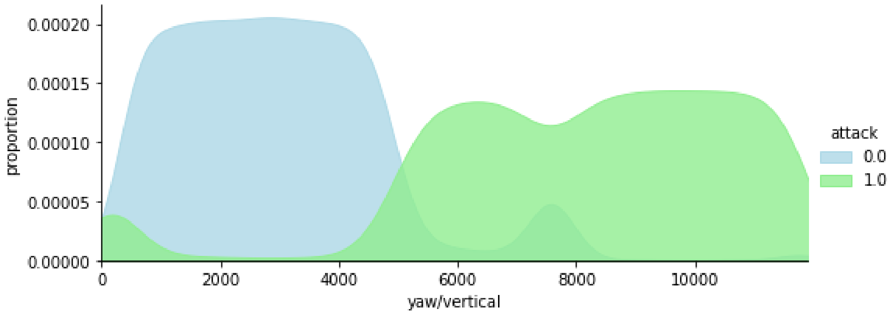

Figure 9. Numerical feature analysis of attacked vertical and yaw motions.

Second, we analyzed the performance of the applied AI models with respect to predicting cyberattacks for commercial UAM. From Figure 10, it is at most clear that KNN predicted successfully the attacks in UAM. Furthermore, the KNN model also predicted the true positive and true negatives of the attack data and no attack data, as is shown in Figure 10. Figure 11 illustrates that the prediction from the logistic regression model was not entirely correct. Additionally, Figure 11 demonstrates that the model predicted the true positive class correctly but could not predict the true negatives. In that case, the logistic regression model incorrectly predicted the negative class. From Figure 12, it is evident that the random forest classifier accurately predicted the attacks in UAM by the attackers. In addition, the random forest classifier model predicted genuine true positive and true negative values for the attack data and no attack data, as depicted in Figure 12. In Figure 13, the random forest classifier correctly predicted the attackers' strikes against UAM. In addition, as indicated in Figure 13, the decision tree classifier model accurately predicted the real true positive and true negative values for the attack data and no attack data. Figure 14 implies that the LSTM model could not successfully predict the accuracy of the attacks on UAM. Additionally, it reveals that the model accurately identified the true positive class but could not predict the true negatives. Therefore, the logistic regression model incorrectly predicted the negative class.

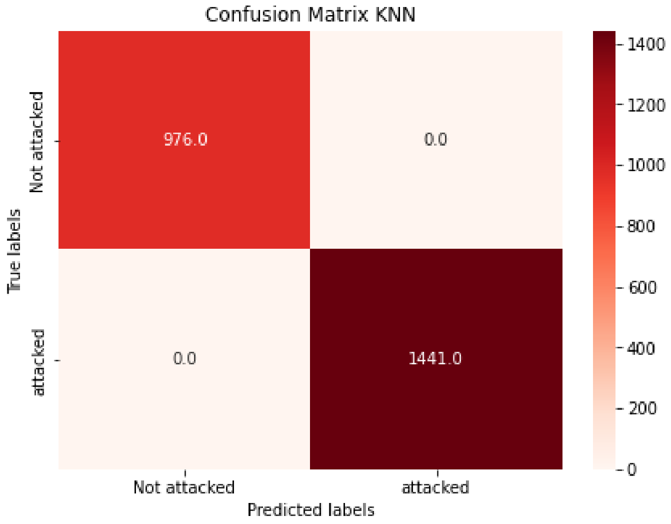

Figure 10. Confusion matrix on prediction of K-nearest neighbors (KNN) classifier.

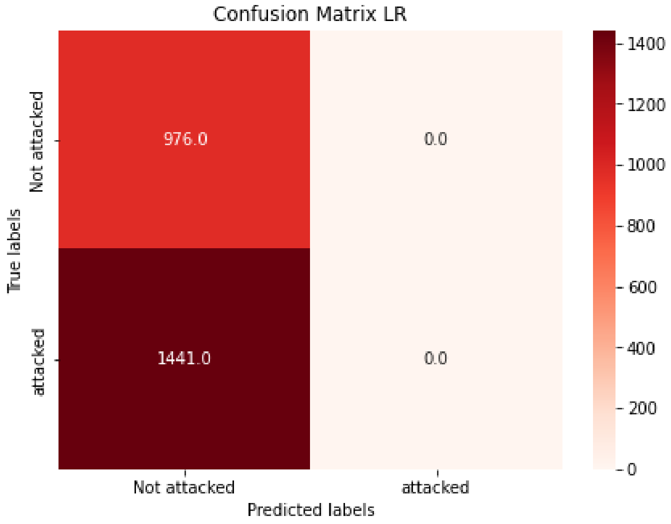

Figure 11. Confusion matrix on prediction of logistic regression classifier.

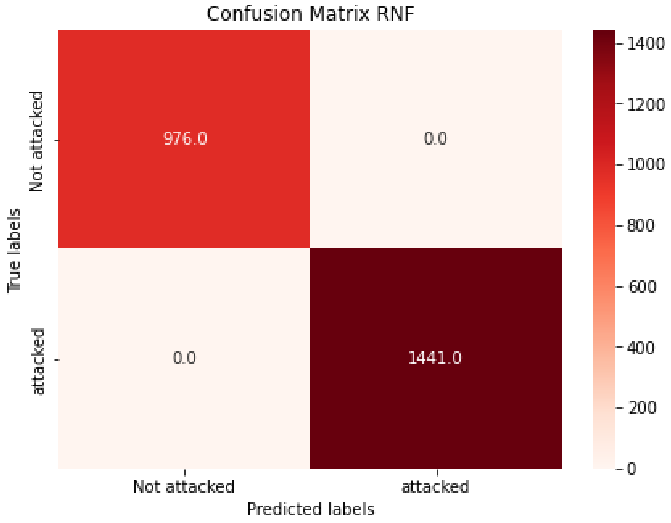

Figure 12. Confusion matrix on prediction of random forest classifier.

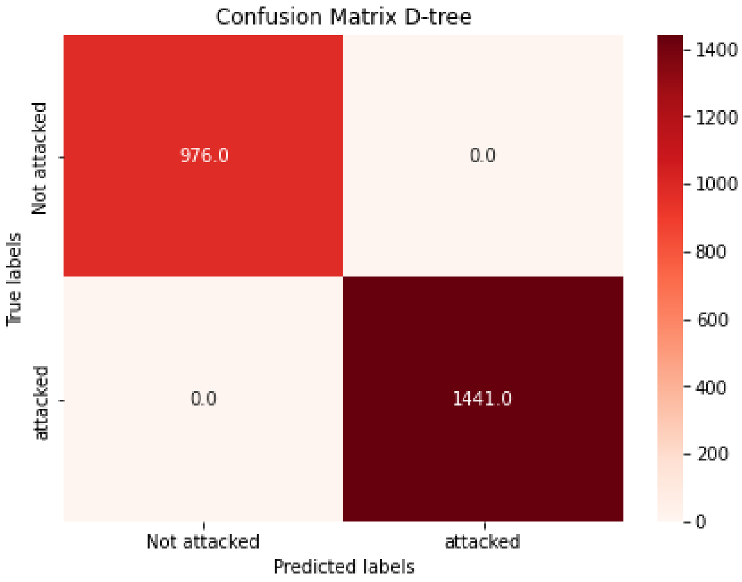

Figure 13. Confusion matrix on prediction of decision tree classifier.

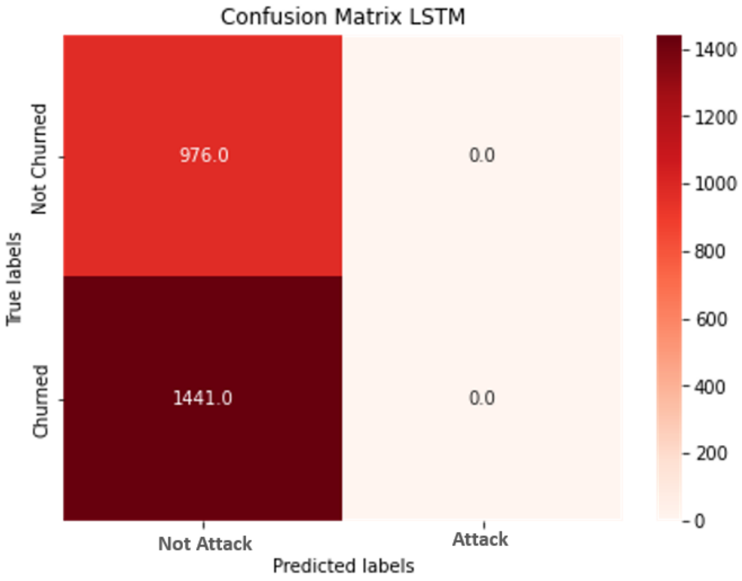

Figure 14. Confusion matrix on prediction of LSTM.

Then, we analyzed the impact of detected cyber threats on the parameters of the switching state (px4io) and radio status of the UAVs. In particular, we analyzed the characteristics of the servo rail voltage and RSSI pin voltage for jamming, spoofing, and benign cases. Furthermore, we analyzed the parameters of the RSSI, remote RSSI, transmit buffer, noise, and remote noise effect on jamming, spoofing, and benign cases. Figure 15 shows the impact of the RSSI voltage on the switching states during jamming and spoofing attacks via the developed exploratory framework. A higher value for the RSSI voltage caused a powerful attack in UAV operation, since the control of the UAV was jammed by the attacker. Figure 16 shows the pair plot analysis between the attack and radio status signal. This correlation indicates the possibility of a strong attack in the received signal strength indicator and remote RSSI. Figure 16 also provides evidence that the attack takes place in the received signal strength indicator as well as the remote RSSI.

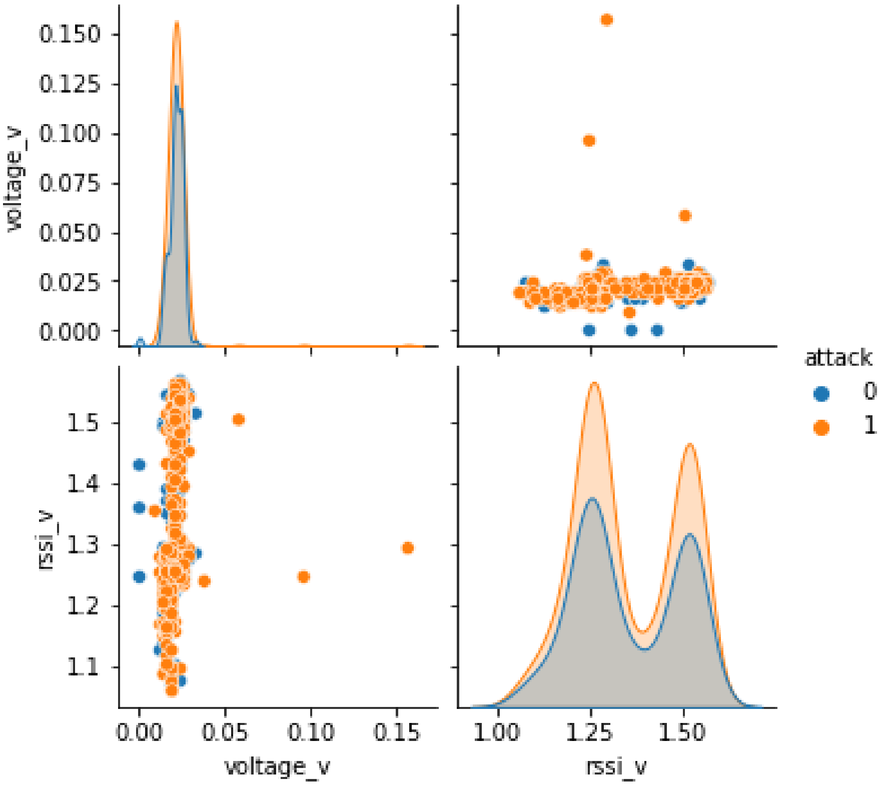

Figure 15. Impact of switching states and received signal indicator of switching states on cyberattack status.

In our experiment, we first ran 50 epochs with a batch size of 75, and after that, we again ran 100 epochs with a batch sizes of 155 in KNN, logistic regression, random forests, decision trees, and LSTM for the training accuracy. However, from both cases, we obtained from the KNN, random forest, and decision tree classifiers 99.99% accuracy, while, from logistic regression and LSTM, we obtained only 40% accuracy, as shown in Table 2.

Table 2. Accuracy comparison among the AI models during jamming and spoofing attack prediction.

AI Model	Precision	Recall	F1-Score	Accuracy (%)
KNN	1	1	1	100
Logistic regression	0.40	1	0.58	40
Random forest	1	1	1	100
Decision tree	1	1	1	100
LSTM	0.40	0.52	0.45	40

A comparison between this work and the previous literature with respect to attack detection is illustrated in Table 3. Table 3 indicates that the decision tree, random forest, and KNN schemes achieved higher precision, recall, and F1-scores compared with the literature [23,28,29] on the UAV frame Holybro S500 dataset. Furthermore, the works of J. Whelan et al. [23], S. I. Ajakwe et al. [28], and J. Whelan et al. [29] considered single-class classification spoofing, jamming, and benign traffic. However, this work considered a combined dataset of spoofing, jamming, and benign cases for detecting cyber threats that can reduce the computational overhead of executing individual classifiers in the literature [23,28,29]. Additionally, the literature [23,28,29] does not provide the exploratory capability of the detected threats. In this work, the proposed cyber-physical safety analyzer can detect all kinds of attacks such as jamming and spoofing from the attitude control systems and explain the root cause of radio frequency-based communication signals. To this end, the developed AI-enabled exploratory cyber-physical safety analyzer framework can successfully predict potential cyberattacks on civilian UAVs. The developed framework also finds the cause of a potential cyberattack using the exploratory capability. Thus, the proposed AI-enabled exploratory cyber-physical safety analyzer framework can reduce the risk of cyberattacks on commercial UAM operations as well as protect UAVs from thieves.

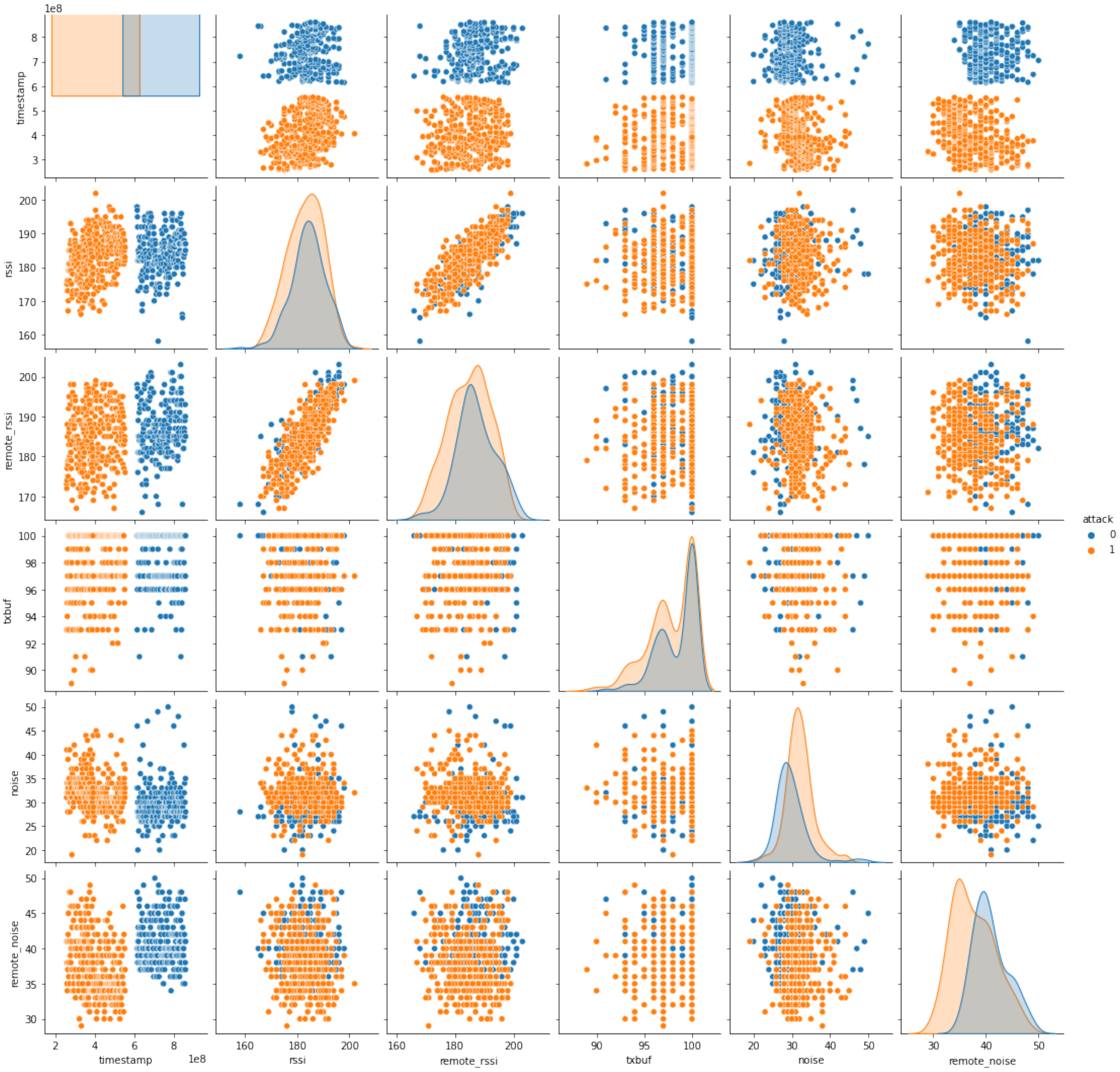

Figure 16. Pair plot analysis between attack and radio status.

In the future, the proposed framework can be extended by deploying a reinforcement learning-based mechanism to capture the dynamic patterns of cyber threats. In other words, the nature of cyber threats evolves. Thus, to protect UAV operation from such new kinds of threats, we also need to deploy the evolving capability of the system. Therefore, we will extend this research in such a way that the system can adapt to the new environment and be capable of detecting and analyzing the dynamic behavior of cyber threats.

Table 3. Comparison between this work and the previous literature on attack detection.

Reference	AI Model	Precision	Recall	F1-Score	Case
This Work	KNN	1	1	1	Spoofing or Jamming, Benign
This Work	Logistic regression	0.40	1	0.58	Spoofing or Jamming, Benign
This Work	Random forest	1	1	1	Spoofing or Jamming, Benign
This Work	Decision tree	1	1	1	Spoofing or Jamming, Benign
This Work	LSTM	0.40	0.52	0.45	Spoofing or Jamming, Benign
J. Whelan et al. [23]	Support vector machine	0.69	0.96	0.80	Spoofing (Malicious)
J. Whelan et al. [23]	Support vector machine	0.99	0.99	0.99	Spoofing (Benign)
J. Whelan et al. [23]	Local outlier factor	0.04	1	0.08	Spoofing (Malicious)
J. Whelan et al. [23]	Local outlier factor	1	0.57	0.72	Spoofing (Benign)
J. Whelan et al. [23]	Auto encoder neural network	0.64	0.99	0.78	Spoofing (Malicious)
J. Whelan et al. [23]	Auto encoder neural network	0.99	0.98	0.99	Spoofing (Benign)
S. I. Ajakwe et al. [28]	Support vector machine	NA	NA	0.81	Spoofing (Malicious)
S. I. Ajakwe et al. [28]	Support vector machine	NA	NA	0.99	Spoofing (Benign)
S. I. Ajakwe et al. [28]	Local outlier factor	NA	NA	0.08	Spoofing (Malicious)
S. I. Ajakwe et al. [28]	Local outlier factor	NA	NA	0.73	Spoofing (Benign)
S. I. Ajakwe et al. [28]	Autoencoder neural network	0.69	0.99	0.85	Spoofing (Malicious)
S. I. Ajakwe et al. [28]	Autoencoder neural network	0.99	0.99	0.99	Spoofing (Benign)
J. Whelan et al. [29]	Support vector machine	1.00	0.66	0.80	Spoofing (Malicious)
J. Whelan et al. [29]	Support vector machine	0.94	1	0.97	Spoofing (Benign)
J. Whelan et al. [29]	Local outlier factor	0.92	0.76	0.83	Spoofing (Malicious)
J. Whelan et al. [29]	Local outlier factor	0.96	0.98	0.97	Spoofing (Benign)
J. Whelan et al. [29]	Auto encoder neural network	0.74	0.96	0.84	Spoofing (Malicious)
J. Whelan et al. [29]	Auto encoder neural network	0.99	0.94	0.97	Spoofing (Benign)
J. Whelan et al. [29]	Support vector machine	0.98	0.07	0.13	Jamming (Malicious)
J. Whelan et al. [29]	Support vector machine	0.99	0.99	0.99	Jamming (Benign)
J. Whelan et al. [29]	Local outlier factor	0.98	0.46	0.63	Jamming (Malicious)
J. Whelan et al. [29]	Local outlier factor	0.86	0.99	0.92	Jamming (Benign)
J. Whelan et al. [29]	Auto encoder neural network	0.84	0.99	0.91	Jamming (Malicious)
J. Whelan et al. [29]	Auto encoder neural network	0.99	0.94	0.97	Jamming (Benign)

6. Conclusions

In this article, we proposed a new AI-enabled exploratory cyber-physical safety analyzer framework for protecting civilian UAVs from theft and crashes due to cyberattacks, such as jamming and spoofing. On top of the proposed framework, we applied numerous AI algorithms such as decision trees, random forests, logistic regression, KNN, and LSTM for predicting cyber threats by analyzing the operational control message of UAM attitude control. Then, we tested the trained model and analyzed the root causes of such cyberattacks with respect to the radio status and switching state of UAM communication by devising a Pearson's correlation coefficient-based statistical analyzer on the proposed framework based on the outcomes of the AI models. Our experiment results showed around 99.99% accuracy in detecting jamming and spoofing by the decision tree, random forest, and KNN schemes. Furthermore, the developed exploratory cyber-physical safety analyzer framework can efficiently determine the root causes of attacks that are taking place by jamming and spoofing through RSSI, remote RSSI, and voltage fluctuations. In summary, compared with the literature, this work achieved higher precision, recall, and F1-scores for detecting jamming and spoofing with the decision tree, random forest, and KNN schemes. The root cause analyzer of the attack becomes the new analogy for protecting civilian UAVs from cyber threats. In the future, we will develop a reinforcement learning-based mechanism for adapting to the dynamic cyberattack environment in real time.

Author Contributions: Conceptualization, investigation, methodology, development, validation, visualization, and writing—original draft M.S.M. and S.H.D.; formal analysis, M.S.M., K.H. and T.I.; writing—review and editing, K.H., T.I. and S.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Yahuza, M.; Idris, M.Y.; Ahmedy, I.B.; Wahab, A.W.; Nandy, T.; Noor, N.M.; Bala, A. Internet of drones security and privacy issues: Taxonomy and open challenges. *IEEE Access* **2021**, *9*, 57243–57270. [CrossRef]
2. Wang, C.-N.; Yang, F.-C.; Vo, N.T.M.; Nguyen, V.T.T. Wireless Communications for Data Security: Efficiency Assessment of Cybersecurity Industry—A Promising Application for UAVs. *Drones* **2022**, *6*, 363. [CrossRef]
3. Tsao, K.Y.; Girdler, T.; Vassilakis, V.G. A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks. *Ad Hoc Netw.* **2022**, *23*, 102894. [CrossRef]
4. Aloqaily, M.; Hussain, R.; Khalaf, D.; Slehat, D.; Oracevic, A. On the role of futuristic technologies in securing UAV-supported autonomous vehicles. *IEEE Consum. Electron. Mag.* **2022**, *11*, 93–105. [CrossRef]
5. Shrestha, R.; Omidkar, A.; Roudi, S.A.; Abbas, R.; Kim, S. Machine-Learning-Enabled Intrusion Detection System for Cellular Connected UAV Networks. *Electronics* **2021**, *10*, 1549. [CrossRef]
6. Ok, M.; Ok, S.; Park, J.H. Estimation of Vehicle Attitude, Acceleration, and Angular Velocity Using Convolutional Neural Network and Dual Extended Kalman Filter. *Sensors* **2021**, *21*, 1282. [CrossRef] [PubMed]
7. Whelan, J.; Almehmadi, A.; Braverman, J.; El-Khatib, K. Threat Analysis of a Long Range Autonomous Unmanned Aerial System. In Proceedings of the 2020 International Conference on Computing and Information Technology (ICCIT-1441), Tabuk, Saudi Arabia, 9–10 September 2020; pp. 1–5. [CrossRef]
8. Rugo, A.; Ardagna, C.A.; Ioini, N.E. A Security Review in the UAVNet Era: Threats, Countermeasures, and Gap Analysis. *ACM Comput. Surv. (CSUR)* **2022**, *55*, 1–35. [CrossRef]
9. Rokach, L.; Maimon, O. Decision trees. In *Data Mining and Knowledge Discovery Handbook*; Springer: Boston, MA, USA, 2005; pp. 165–192.
10. Breiman, L. Random forests. *Mach. Learn.* **2001**, *45*, 5–32.
11. Kleinbaum, D.G.; Dietz, K.; Gail, M.; Klein, M.; Klein, M. *Logistic Regression*; Springer: New York, NY, USA, 2002.
12. Guo, G.; Wang, H.; Bell, D.; Bi, Y.; Greer, K. KNN model-based approach in classification. In Proceedings of the OTM Confederated International Conferences "On the Move to Meaningful Internet Systems", Rhodes, Greece, 21–25 October 2003; Springer: Berlin/Heidelberg, Germany, 2003; Volume 3, pp. 986–996.
13. Yu, Y.; Si, X.; Hu, C.; Zhang, J. A review of recurrent neural networks: LSTM cells and network architectures. *Neural Comput.* **2019**, *31*, 1235–1270. [CrossRef] [PubMed]
14. Whelan, J.; Sangarapillai, T.; Minawi, O.; Almehmadi, A.; El-Khatib, K. UAV Attack Dataset [Internet]. *IEEE Dataport* **2020**. [CrossRef]
15. Benesty, J.; Chen, J.; Huang, Y.; Cohen, I. Pearson correlation coefficient. In *Noise Reduction in Speech Processing*; Springer: Berlin/Heidelberg, Germany, 2009, pp. 1–4.
16. Krishna, C.G.L.; Murphy, R.R. A review on cybersecurity vulnerabilities for unmanned aerial vehicles. In Proceedings of the 2017 IEEE International Symposium on Safety, Security and Rescue Robotics (SSRR), Shanghai, China, 11–13 October 2017; pp. 194–199. [CrossRef]
17. Bekmezci, I.; Sahingoz, O.K.; Temel, S. Flying ad-hoc networks (FANETs): A survey. *Ad Hoc Netw.* **2013**, *11*, 1254–1270. [CrossRef]
18. Bekmezci, I.; Senturk, E.; Turker, T. Security issues in flying ad-hoc networks (FANETS). *J. Aeronaut. Space Technol.* **2016**, *9*, 13–21.
19. Xu, W.; Ma, K.; Trappe, W.; Zhang, Y. Jamming sensor networks: attack and defense strategies. *IEEE Netw.* **2006**, *20*, 41–47. [CrossRef]
20. Su, J.; He, J.; Cheng, P.; Chen, J. A stealthy GPS spoofing strategy for manipulating the trajectory of an unmanned aerial vehicle. *IFAC-PapersOnLine* **2016**, *49*, 291–296. [CrossRef]
21. Javaid, A.Y.; Jahan, F.; Sun, W. Analysis of global positioning system-based attacks and a novel global positioning system spoofing detection/mitigation algorithm for unmanned aerial vehicle simulation. *Simulation* **2017**, *93*, 427–441. [CrossRef]
22. Mitchell, R.; Chen, I.R. Adaptive intrusion detection of malicious unmanned air vehicles using behavior rule specifications. *IEEE Trans. Syst. Man, Cybern. Syst.* **2013**, *44*, 593–604. [CrossRef]
23. Whelan, J.; Sangarapillai, T.; Minawi, O.; Almehmadi, A.; El-Khatib, K. 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 (Q2SWinet '20), Alicante, Spain, 16–20 November 2020; Association for Computing Machinery: New York, NY, USA, 2020; pp. 23–28. [CrossRef]
24. Kwon, C.; Yantek, S.; Hwang, I. Real-Time Safety Assessment of Unmanned Aircraft Systems against Stealthy Cyber Attacks. *J. Aerosp. Inf. Syst.* **2015**, *13*, 27–45. [CrossRef]

25. Borri, A.; Bianchi, D.; Di Benedetto, M.D.; Di Gennaro, S. Vehicle attitude control with saturating actuators: Workload balancing and reference adaptation. In Proceedings of the 52nd IEEE Conference on Decision and Control, Firenze, Italy, 10–13 December 2013; Volume 10, pp. 1558–1563.
26. Scikit-Learn. Supervised Learning. Available online: https://scikit-learn.org/stable/ (accessed on 10 October 2022).
27. Scikit-Learn. sklearn.model_selection.GridSearchCV. Available online: https://scikit-learn.org/stable/modules/generated/sklearn.model_selection.GridSearchCV.html (accessed on 24 December 2022).
28. Ajakwe, S.O.; Ihekoronye, V.U.; Kim, D.S.; Lee, J.M. Pervasive Intrusion Detection Scheme to Mitigate Sensor Attacks on UAV Networks. In Proceedings of the 2022 Summer Conference of the Korean Society of Communications and Communications, Jeju Island, Republic of Korea, 19–21 October 2022; pp. 1267–1268.
29. Whelan, J.; Almehmadi, A.; El-Khatib, K. Artificial intelligence for intrusion detection systems in unmanned aerial vehicles. *Comput. Electr. Eng.* **2022**, *99*, 107784. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.