2023 International Conference on Computing, Networking and Communications (ICNC): Communications and Information Security Symposium

A Hybrid Delay-aware Approach towards UAV Flight Data Anomaly Detection

Mengjie Jia, Ashok Raja, Jiawei Yuan
Department of Computer and Information Science
University of Massachusetts Dartmouth
Emails: mjia@umassd.edu, araja1@umassd.edu, jyuan@umassd.edu

2023 International Conference on Computing, Networking and Communications (ICNC) | 978-1-6654-5719-4/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICNC57223.2023.10074138

***Abstract*—With the rapid development of unmanned aerial vehicle (UAV) technologies, UAVs are now increasingly leveraged to perform military and civilian tasks today. Meanwhile, as a complex cyber-physical system, UAVs are also facing security and reliability concerns raised by internal systems errors and external cyber-attacks from multiple aspects. Recent research has spent efforts on leveraging AI and machine learning techniques to predict the flying status of UAVs using their flight data for anomaly detection. However, these methods often ignore the prediction delay existing in status-changing periods during the UAV's operation, which inevitably causes false alarms and opens a window for malicious adversaries if they are not appropriately addressed. In this paper, we propose a new approach to enable effective anomaly detection and recovery for UAV flight data. Our approach adopts a hybrid design to eliminate false alarms during the status-changing periods while maintaining the high reliability of anomaly detection. We evaluate the proposed approach on flight data collected from multiple UAV flight paths. Our evaluation results validate the effectiveness of our hybrid design, which achieves both high anomaly detection accuracy and reliable recovery.**

I. Introduction

Recent years have witnessed the rapid development of UAVs in various military and civilian application scenarios, such as remote sensing, infrastructure inspection, and intelligence, surveillance, and reconnaissance (ISR) [1]–[3]. Along with the widespread adoption of UAVs, its security and reliability has also received increasing attention from both academia and industry considering the potential internal failures and external attacks [4], [5]. The abnormal flying status of a UAV not only affects its own mission but can also cause severe public safety consequences.

To improve the reliability of UAVs, multiple research attempts have been made to enable anomaly detection and recovery by analyzing the UAV's flight data [6]–[13]. This is because the flight status of a UAV can be directly reflected by the flight data collected from its sensors. Approaches proposed in existing research can be mainly classified into two categories, i.e., model-based [6]–[8] and model-free [9]–[13]. The model-based approaches treat the UAV control process as a white box and use techniques from control theory for detection. Differently, the model-free approaches consider the control process as a black box and leverage AI and machine learning techniques to classify abnormal statuses. This paper focuses on the model-free design, which has become a prevalent trend in recent research to handle both known abnormal patterns and unknown faults. In particular, the state-of-the-art research increasingly adopts long short-term memory (LSTM) structure in the design of model-free UAV anomaly detection approaches [11]–[13], because the time-series nature of UAV flight data makes LSTM become an excellent fit to discover their spatio-temporal correlation.

Although these recent approaches [11]–[13] have been demonstrated to be effective overall for the anomaly detection of UAV flight data, they still suffer from high false-positive rates at time windows after flight status changes (e.g., turning). Specifically, the real-time change of flying status of a UAV triggers immediate changes in the reading of related sensors. However, the corresponding prediction made by the deep learning models can be delayed since the flight data trend right before the UAV status change is typically different. Such a delay introduces notable gaps between the actual sensor reading and predicted sensor values, which further leads to false alarms if these gaps exceed the threshold defined for anomaly detection. Fig.1 presents an example we evaluated using the approach proposed in [12], which shows obvious gaps between the roll angle values from actual sensor reading and prediction right after a turning is made by the UAV. In real-time anomaly detection for UAVs, such false alarms can be eliminated by temperately increasing the threshold for these flight status-changing periods, nevertheless, it will also restrict the detection of true anomalies in these periods and open windows for malicious adversaries to inject manipulated data.

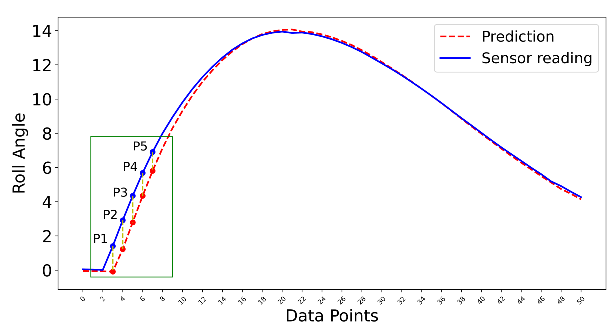

Fig. 1. Example of Prediction Delay in UAV Turning

In this paper, we propose an effective real-time anomaly detection approach for UAV flight data, which adopts a hybrid design to overcome the limitation introduced by the prediction delay. To be specific, our approach separates the flight data of UAVs into the non-status-changing period and the status-changing period, in which the status-changing period is the time window that prediction delays are likely to happen due to the change of flying status. An LSTM-based DNN model driven by multi-sensor inputs is adopted in our approach for anomaly detection during the non-status-changing period. With regard to the status-changing period, an alternative anomaly detection design is adopted using pre-computed reference data and a separate DNN model to resolve the negative impacts introduced by the prediction delay. We implement and evaluate our proposed approach on multiple real-time UAV flying patterns generated using PX4 autopilot [14]. The evaluation results show that our approach achieves high accuracy for anomaly detection in both non-status-changing periods and status-changing periods. Compared with existing research that uses a single DNN model for anomaly detection, our hybrid approach significantly reduces the false-positive rate without sacrificing the reliability of anomaly detection. Our results also demonstrate that our approach supports reliable recovery from the abnormal status for UAVs thanks to the accurate prediction achieved by our hybrid design.

The rest of the paper is organized as follows: In Section II, we review and discuss related works. Section III presents the detailed construction of our proposed approach for UAV anomaly detection. We evaluate and discuss our approach in Section IV, which is followed by the conclusion in Section V.

II. Related Works

Existing research efforts on anomaly detection of UAVs' flight data can be mainly classified into two categories, including the model-based method [6]–[8] and the model-free method [9]–[13]. The model-based method usually uses Kalman Filters to predict future data based on uncertain measurements from sensors and previous estimations. Ivan and Nabil [6] applied an unscented Kalman Filter (UKF) with Gaussian process adaption to detect the fault status in UAVs' inertial navigation system. In order to achieve faster response and lower computation load in fault detection, Liu *et al.* [7] proposed an adaptive estimation method using a bank of UKFs running in parallel for monitoring the actuators' status in a UAV. Guo *et al.* [8] developed a fault detection approach for airspeed using an extended Kalman Filter (EKF) to estimate the airspeed with multiple sensors. Their approach is independent of the airspeed measurements and can be moved to other aircraft with no need to change the filter process. Although Kalman Filters can keep tracking the status of navigation and control systems, the estimation accuracy of this method depends on the corresponding physical model.

Compared with the model-based method, the model-free design can learn the pattern of training data without the information and knowledge of the mechanical system. The classification and regression models used in a model-free method are usually trained on the normal flight data due to the lack of faulty data, which is rare and expensive to acquire in the real world. To address this inevitable imbalance problem in dataset, Edward *et al.* [9] used a one-class SVM learning the normal data pattern to detect and assess the outliers and abnormal status of an individual aircraft during the descent period. Li *et al.* [10] presented a cluster-based anomaly detection approach to detect the abnormal flights of commercial aircraft, which outperformed the multiple kernel anomaly detection algorithm in the detection of continuous flight parameters. These approaches mentioned above are non-parametric learning methods and have limited ability to learn and extract the representation from high-dimensional data. To deal with this problem, Zhong *et al.* [11] introduced a spatio-temporal correlation based anomaly detection method for high-dimensional flight data. They first used an artificial neural network for spatio-temporal correlation analysis to select the most correlated flight parameters with the monitored sensor, which are used as the inputs of an LSTM regression model for estimation. Wang *et al.* [12] designed a regression model based on LSTM networks with residual filtering to avoid random noise for the fault detection and recovery of flight data from UAVs. The results of their experiment demonstrate that their model can reduce the effect of random noise in flight data and improve the detection sensitivity to minor faults. When it comes to the detection for multiple parameters, running multiple single-output LSTM networks, where each LSTM is responsible for one parameter, can cause too much redundancy and is time-consuming as well. To solve this issue, Ahmad and Zouhair [13] proposed a multi-output convolutional LSTM for multivariate anomaly detection of UAV flight data, which combines convolutional neural networks (CNN) and LSTM to achieve sequence-to-sequence prediction. They claimed their approach is more suitable and faster in analyzing and detecting the multivariate flight data. These existing methods adopt a single model to detect the abnormal status of UAV for the entire flight path, and hence the effectiveness becomes restricted during the flight status-changing period.

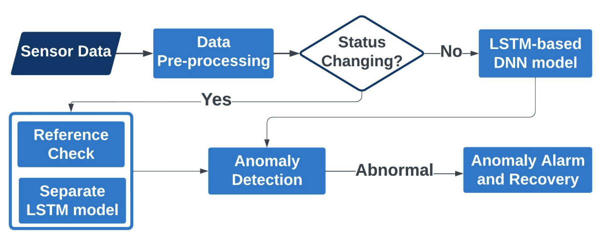

Fig. 2. Framework of LSTM-based Detection System

III. Construction

The overall architecture of our anomaly detection approach for UAV flight data is presented in Fig.2. During the UAV's operation, data from selected sensors are continuously fed into our approach for pre-processing, including data normalization and data construction with sliding windows. To determine the abnormal status of a sensor reading at time t, our hybrid approach first selects the data analysis procedure based on whether t falls into status-changing periods or not. For non-status-changing periods, an LSTM-based DNN model is adopted to predict the sensor value at t with sensors inputs from the sliding window before t. For status-changing periods, we adopt a delay-mitigation procedure to predict the sensor value at t with a reference check design and a separate regression model. Finally, the predicted sensor value at t will be compared with the actual sensor reading data using a pre-defined threshold to determine whether the sensor data is abnormal or not, and the abnormal sensor data will be recovered. We now present the detailed construction of each procedure in our approach.

TABLE I
LIST OF SENSOR PARAMETERS

Roll Angle	Actuator Yaw Angle
Pitch Angle	Roll Rate
Yaw Angle	Pitch Rate
Actuator Roll Angle	Yaw Rate
Actuator Pitch Angle	Airspeed

A. LSTM-based DNN Anomaly Detection

Given the fact that a UAV system is equipped with various sensors and many of them are correlated with each other to some extent, our approach combines inputs from correlated sensors when predicting the value of a selected sensor for anomaly detection. In this paper, we focus on anomaly detection by analyzing roll angle data, which is one of the important parameters to reflect the safe operation of UAVs and has been widely adopted for anomaly detection [12], [13], [15], [16]. 9 additional collaborated sensor parameters to the roll angle are included to support the analysis as summarized in Table I.

During the pre-processing, raw sensor inputs at each time point t is first processed using min-max normalization and denoted as

$$\boldsymbol{V_t} = \left(s_{1,t}, s_{2,t}, \ldots, s_{n,t}\right), \boldsymbol{V_t} \in \mathbb{R}^{n\times 1}$$

where $s_{i,t}, 1 \leq i \leq n$ is the value of the i-th sensor at time t. To predict the sensor value at time t, a sliding window of grouped sensor input sequences before t will be fed into the DNN model, which is denoted as

$$\boldsymbol{X_t} = \left(\boldsymbol{V_{t-m}}, \boldsymbol{V_{t-m+1}}, \ldots, \boldsymbol{V_{t-1}}\right), \boldsymbol{X_t} \in \mathbb{R}^{n\times m}, t > m$$

where m is the length of sliding window. The DNN model consists of two stacked LSTM layers, a fully connected layer, and an output layer as depicted in Fig.3.

During the real-time anomaly detection, the UAV utilizes the pre-trained DNN model with $\boldsymbol{X_t}$ as the input at time t and obtains a predicted roll angle value $\hat{y}_t$. An error e_t between the predicted value $\hat{y}_t$ and actual sensor reading y_t is calculated with a low-pass infinite impulse response (IIR) filter as

$$\begin{cases} \alpha = |y_t - \hat{y}_t| & \\ e_t = \alpha & \text{if } t = 0 \\ e_t = \alpha + \beta(e_{t-1} - \alpha) & \text{otherwise} \end{cases}$$

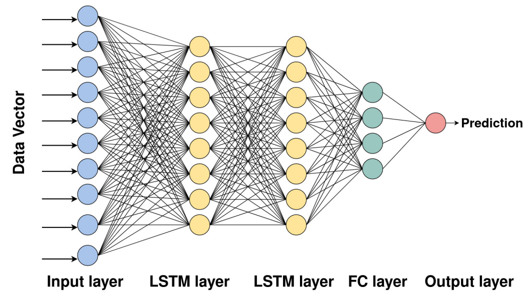

Fig. 3. Architecture of LSTM-based DNN Model

The IIR filter is applied to avoid the fluctuations caused by noises and β is the filter coefficient. The sensor reading y_t is considered as abnormal is the error e_t is greater than the pre-defined anomaly threshold.

In our design, the anomaly threshold is calculated based on the filtered errors between the predicted values and the corresponding target values obtained during the training of the DNN model as $Threshold = \mu + k \times \sigma$, where μ and σ are the mean value and standard deviation of the filtered training errors respectively, and k is a constant that can be adjusted to get an acceptable threshold to optimize anomaly detection performance.

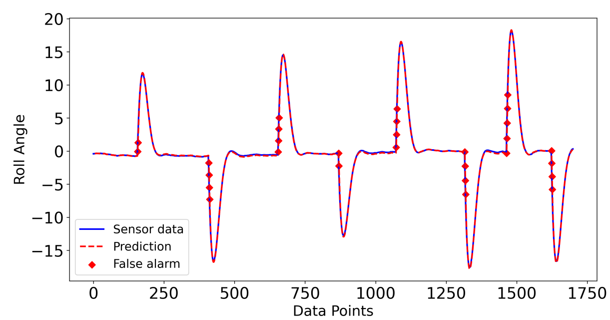

Fig. 4. Example of False Alarms in Status-changing Periods

B. Delay-aware Anomaly Detection for Status-changing Periods

Although the LSTM-based DNN anomaly detection can effectively handle non-status-changing periods, its performance struggles during the status-changing periods due to the delay in its prediction. As an example shown in Fig.4, such a delay introduces multiple false alarms for each status-changing period caused by the turning of a UAV. Therefore, instead of using the prediction values from the LSTM-based DNN model for overall anomaly detection as reference points, new effective references shall be identified for these status-changing periods.

In our design, two types of reference points are introduced for status-changing periods. First, we pre-compute and store reference data of the targeted sensor for the first r time points, which can be estimated using the average values obtained from offline experiments for the same status change under different flying patterns. Although such an estimation is not likely to be exactly the same as the actual sensor reading in the real-time analysis due to different environmental factors and system noises, their difference still has a high possibility to be bounded by the pre-defined threshold and hence significantly reduces the false positive rate. In addition, a separate LSTM-based DNN model is trained specifically using data from status-changing periods, which takes sensor inputs from a sliding window of r time points. Therefore, the DNN model is used for anomaly detection after the first r time points in the status-changing period. The value of r is determined by the input of the DNN model to enable effective anomaly detection, which is set as $r = 3$ according to our experimental analysis.

During the UAV operation, its flying status change is associated with the corresponding control command. Therefore, when a status change control command is received or the planned command is triggered, the UAV system will switch to the delay-aware anomaly detection strategy for a short time period until the delay has been mitigated.

C. Recovery from Abnormal Status

The abnormal detection in our proposed approach relies on the real-time prediction from DNN models and pre-computed reference data. In particular, when the sensor data is identified as abnormal, it will be replaced with the corresponding prediction value or reference data for recovery. After that, the UAV system will adopt the recovery value for further UAV operations and anomaly detection.

IV. Evaluation

A. Experiment Setup

In our experiment, we simulated 10 different UAV flight paths using PX4 autopilot [14] and QGroundControl [17], which involve different status-changing periods. Data from 10 sensor parameters as described in Table I are collected for the anomaly detection of the UAV's roll angle data. By setting the sliding window size as 5, our dataset consists of $3,000$ sliding windows of sensor data for training after reformulation and normalization. In our training, the batch size is set as 16 and the number of epochs is 300. The test dataset has 1700 data points, in which 200 abnormal data points are randomly injected as shown in Fig.5.

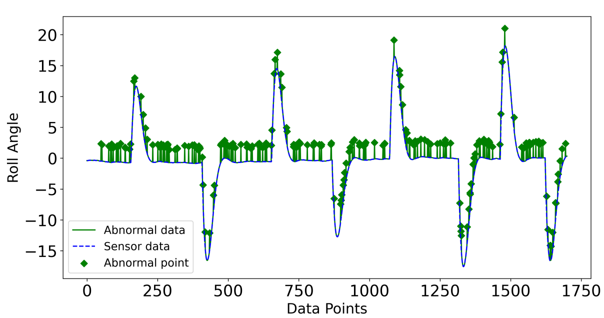

Fig. 5. Normal roll angle and Abnormal roll angle

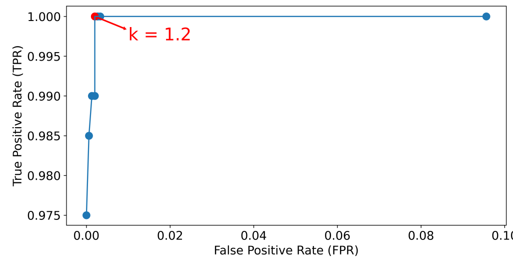

Fig. 6. ROC Curve

We use Mean Square Error (MSE) and Mean Absolute Error (MAE) for regression evaluation, which can be calculated by

$$MSE = \frac{1}{n}\sum_{i=1}^{n}(y_i - \hat{y}_i)^2 \qquad MAE = \frac{1}{n}\sum_{i=1}^{n}|y_i - \hat{y}_i|$$

MSE indicates how the prediction results deviate from the target values and MAE reflects the prediction error directly. True positive rate (TPR), false positive rate (FPR), false negative rate (FNR), and true negative rate (TNR) are used to measure the accuracy of anomaly detection.

B. Results

As the selection of threshold plays a critical role in the effectiveness of anomaly detection, we first evaluate our proposed approach using different thresholds to balance the trade-off between TPR and FPR. In our evaluation, we set filter coefficient $\beta = 0.1$ and vary the value k from 1 to 2 with a step of 0.1. As the ROC curve shown in Fig.6, optimized thresholds can be obtained when k is in the range of [1.1, 1.6]. In the rest of our evaluation, the threshold is set to 1.48 with $k = 1.2$ based on the optimized range we obtained.

The evaluation results of our approach in terms of anomaly detection effectiveness are summarized in Table II. We also evaluated the model-free approach proposed in [12] using the same flight path for comparison. As presented in Table II, our proposed hybrid approach is able to detect all abnormal data points while achieving a 0 FPR. As a comparison, while [12] also achieves good performance for the detection of abnormal data points with a $TPR = 0.97$, it suffers from a high FPR at 0.24. The high FPR of [12] is mainly caused by its prediction delay in the status-changing periods as shown in Table II, which reaches 0.79 and can significantly affect the reliability of anomaly detection in these periods. As discussed in Section III-B, such a prediction delay makes the prediction values from the DNN model becomes ineffective to serve as reference data for anomaly detection. Differently, thanks to the hybrid design in our approach, it can successfully eliminate the FPR by handling the delay with adjusted reference data.

In our approach, abnormal data are replaced with the prediction values or reference data for recovery. Therefore, the recovery capability depends on the accuracy of prediction values and reference data generated by our approach. As presented in Table III, our approach achieves low MAE and MSE for both

TABLE II
ANOMALY DETECTION EFFECTIVENESS AND COMPARISON

Anomaly Detection - Overall				
	FPR	FNR	TPR	TNR
Our Approach	0	0	1.0	1.0
[12]	0.24	0.03	0.97	0.76
Anomaly Detection - Status Changing Periods				
	FPR	FNR	TPR	TNR
Our Approach	0	0	1.0	1.0
[12]	0.79	0.17	0.83	0.21

the overall flight path and the status-changing periods, which indicates the accurate prediction for recovery. As shown in Fig.7, while random abnormal data are continuously injected, our approach is able to help the UAV successfully recover from the abnormal status. As a comparison, the prediction accuracy of [12] is significantly reduced during the status-changing periods as indicated by its high MAE and MSE values in these periods shown in Table III.

TABLE III
PREDICTION ACCURACY AND COMPARISON

Regression Evaluation - Overall		
	MAE	MSE
Our Approach	0.1263	0.0590
[12]	0.8139	2.9563
Regression Evaluation - Status Changing Periods		
	MAE	MSE
Our Approach	0.7091	0.6934
[12]	3.5606	15.7858

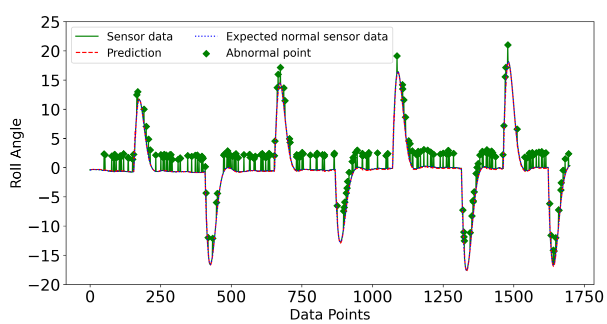

Fig. 7. Example of Abnormal Recovery

V. CONCLUSION

This paper performs a study on anomaly detection and recovery for UAV flight data. Our study first identifies the prediction delay issue in model-free anomaly detection, which can cause high false-positive rates in UAV's status-changing periods. With this observation, this paper then designs a hybrid approach to overcome false alarms during the status-changing periods, which hence enables the UAV to perform accurate anomaly detection and reliable recovery. Our proposed approach is evaluated using different UAV flight paths. A comparison between our approach and existing research is also conducted in our evaluation. The evaluation results demonstrate the effectiveness of our approach in terms of flight data prediction, anomaly detection, as well as recovery from the abnormal status.

ACKNOWLEDGMENT

This work was supported by the US NSF Awards (OAC-2229976 and DGE-1956193) and the UMass Dartmouth Cybersecurity Center Fellowship.

REFERENCES

[1] M. Bhaskaranand and J. D. Gibson. Low-complexity video encoding for uav reconnaissance and surveillance. In *2011 - MILCOM 2011 Military Communications Conference*, pages 1633–1638, Nov 2011.
[2] T. Tomic, K. Schmid, P. Lutz, A. Domel, M. Kassecker, E. Mair, I. L. Grixa, F. Ruess, M. Suppa, and D. Burschka. Toward a fully autonomous uav: Research platform for indoor and outdoor urban search and rescue. *IEEE Robotics Automation Magazine*, 19(3):46–56, Sept 2012.
[3] Inkyu Sa, Stefan Hrabar, and Peter Corke. *Outdoor Flight Testing of a Pole Inspection UAV Incorporating High-speed Vision*, pages 107–121. Springer International Publishing, Cham, 2015.
[4] Riham Altawy and Amr M Youssef. Security, privacy, and safety aspects of civilian drones: A survey. *ACM Transactions on Cyber-Physical Systems*, 1(2):1–25, 2016.
[5] Yueyan Zhi, Zhangjie Fu, Xingming Sun, and Jingnan Yu. Security and privacy issues of uav: a survey. *Mobile Networks and Applications*, 25(1):95–101, 2020.
[6] Ivan Vitanov and Nabil Aouf. Fault diagnosis for mems ins using unscented kalman filter enhanced by gaussian process adaptation. In *2014 NASA/ESA Conference on Adaptive Hardware and Systems (AHS)*, pages 120–126. IEEE, 2014.
[7] Liyuan Liu, Yue Ma, Bin Xu, Changle Xiang, and Xingbang Yang. Fault detection and isolation based on ukfs for a novel ducted fan uav. In *2016 IEEE International Conference on Aircraft Utility Systems (AUS)*, pages 212–218, 2016.
[8] Dingfei Guo, Maiying Zhong, and Donghua Zhou. Multisensor data-fusion-based approach to airspeed measurement fault detection for unmanned aerial vehicles. *IEEE Transactions on Instrumentation and Measurement*, 67(2):317–327, 2017.
[9] Edward Smart, D Brown, and John Denman. Combining multiple classifiers to quantitatively rank the impact of abnormalities in flight data. *Applied Soft Computing*, 12(8):2583–2592, 2012.
[10] Lishuai Li, Santanu Das, R John Hansman, Rafael Palacios, and Ashok N Srivastava. Analysis of flight data using clustering techniques for detecting abnormal operations. *Journal of Aerospace information systems*, 12(9):587–598, 2015.
[11] Jie Zhong, Yujie Zhang, Jianyu Wang, Chong Luo, and Qiang Miao. Unmanned aerial vehicle flight data anomaly detection and recovery prediction based on spatio-temporal correlation. *IEEE Transactions on Reliability*, 71(1):457–468, 2022.
[12] Benkuan Wang, Datong Liu, Yu Peng, and Xiyuan Peng. Multivariate regression-based fault detection and recovery of uav flight data. *IEEE Transactions on Instrumentation and Measurement*, 69(6):3527–3537, 2019.
[13] Ahmad Alos and Zouhair Dahrouj. Using mlstm and multioutput convolutional lstm algorithms for detecting anomalous patterns in streamed data of unmanned aerial vehicles. *IEEE Aerospace and Electronic Systems Magazine*, 37(6):6–15, 2022.
[14] PX4 Autopilot. https://px4.io/.
[15] Haithem Taha and Ahmed Hassan. Nonlinear flight physics of the lie-bracket roll mechanism. 01 2021.
[16] Ahmed M Hassan and Haitham E Taha. A novel airplane roll mechanism: Nonlinear motion planning approach. In *AIAA Scitech 2019 Forum*, page 0912, 2019.
[17] QGroundControl. http://qgroundcontrol.com/.