Sensor Data-Driven UAV Anomaly Detection using Deep Learning Approach

Julio Galvan†, Ashok Raja‡, Yanyan Li†, Jiawei Yuan‡
† *Department of Computer Science and Information Systems, California State University San Marcos, San Marcos, CA, USA*
‡ *Department of Computer & Information Science, University of Massachusetts Dartmouth, North Dartmouth, MA, USA*
galva057@cougars.csusm.edu, araja1@umassd.edu, yali@csusm.edu, jyuan@umassd.edu

MILCOM 2021 - 2021 IEEE Military Communications Conference (MILCOM) | 978-1-6654-3956-5/21/$31.00 ©2021 IEEE | DOI: 10.1109/MILCOM52596.2021.9653036

***Abstract*—Thanks to the high mobility and rich sensing capabilities of unmanned aerial vehicles (UAVs), or drones, they are increasingly leveraged to perform a series of military and civilian tasks today. Meanwhile, UAVs are also facing various security and safety concerns raised by both external attacks and internal hardware/software failures. Therefore, detecting the abnormal status of a UAV is a critical task to protect it against malicious adversaries and prevent potential crashes. In this paper, we propose an anomaly detection system for UAVs by monitoring and analyzing their sensor data in real-time using deep learning approaches. The proposed system leverages the convolutional neural network (CNN) to extract and learn features automatically from raw sensor data and then process them to support anomaly detection. We construct a data set of UAV IMU sensor data using our UAV cybersecurity simulation platform to support the training of our CNN model. Different deep learning models are also evaluated and compared in this paper. We validate the performance of the proposed detection system using extensive experimental evaluation, which demonstrates that our system achieves high detection accuracy under different conditions.**

I. Introduction

In recent years, UAVs have been adopted in a spectrum of military and civilian applications, including remote sensing, search and rescue, infrastructure inspection, and intelligence, surveillance, and reconnaissance (ISR) [1]–[4]. Compared with traditional static sensors, UAVs have clear advantages in coverage, mobility, and easy deployment, which make them extremely suitable for onsite aerial monitoring in both urban and rural areas, especially for these difficult-to-reach areas. Currently, there are over $522,000$ commercial UAVs registered in the United States with the Federal Aviation Administration (FAA), and this number is expected to double by 2024 [5].

As a typical type of cyber-physical system, UAVs face potential security attacks from multiple aspects, including but not limited to control, software, sensors, and communications [6], [7]. Once these external threats have been successfully launched on a UAV, its operation might turn into abnormal status, which can further cause severe consequences. For example, GPS spoofing attacks can mislead the UAV's flying pattern [8] and spoofing attacks on gyroscopic sensors of a UAV through acoustic noises can lead to its crash [9]. In addition, a UAV's operation can also be affected by internal factors, such as defects on UAV parts and software failures. These factors are usually not obvious to identify at beginning, but can cause abnormal status during the operation. For example, a small crack on the propeller of a UAV may not be noticed during the takeoff phase, however, it can gradually affect the operations of the UAV and may even lead to an accident if the crack becomes larger during its flight. Therefore, with the increasing usage of UAVs, it is critical to accurately detect the abnormal status of UAVs in real-time and help prevent attacks and accidents in advance.

To enable the detection of a UAV's abnormal status, we consider analyzing its sensor data in real-time. This is because the status of a UAV greatly relies on the inputs of these sensors. In particular, inertial measurement unit (IMU) sensor is selected in this paper for the following reasons: (1) As an important sensor, IMU is equipped by most UAVs; (2) IMU detects the real-time rate of acceleration as well as the changes in rotational attributes of the UAV, and thus can be leveraged for the real-time monitoring of a UAV's flying status; (3) IMU has a high data generation rate and hence has a high possibility of generating sufficient data points before and after the appearance of abnormal status for detection.

With these factors in mind, this paper aims to explore and investigate how to detect a UAV's abnormal status by capturing and analyzing the corresponding changes in IMU sensor data. In particular, we propose a data-driven approach with deep learning to perform effective and efficient anomaly detection for UAVs, in which a CNN model is constructed and trained to extract and learn features from IMU sensor data for capturing signs of abnormal status. As deep learning approaches have been demonstrated to be effective to learn complex patterns from labeled data sets, we collect and label a high-quality data set to support the training of deep learning models through extensive simulation using our UAV cybersecurity platform. Our data set covers IMU sensor data obtained from normal UAV operations as well as these from abnormal UAV status with different patterns, frequency, duration, and strength. This data set can also be used to support other related research in the community (e.g., IMU-based UAV tracking). Different deep neural network (DNN) models are also examined in this paper to optimize the performance of our anomaly detection system. Our evaluation results demonstrate that our detection system is effective and stable under different conditions.

The rest of our paper is structured as follows: In Section II, we review and discuss related work. Section III introduces the construction of our proposed UAV anomaly detection

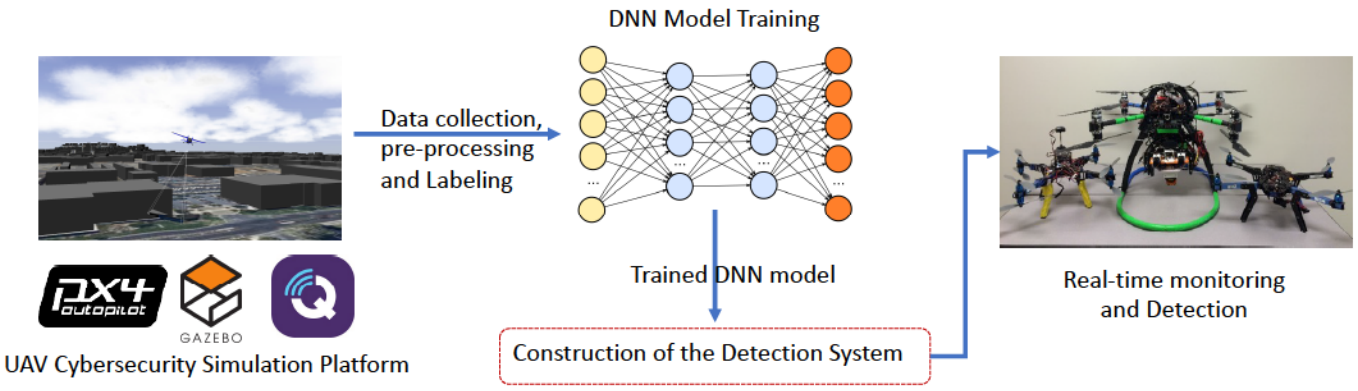

Fig. 1. Construction Overview

system. We evaluate the performance of our detection system in Section IV. We conclude the paper and discuss future work in Section V.

II. Related Work

The problem of anomaly detection for UAVs and other robotic vehicles has attracted many research efforts due to its importance to assure their security and safety [10]–[22]. Existing anomaly detection solutions can be classified into the following categories according to the main techniques they are using, including signature-based, redundancy-based, behavior-based, and learning-based.

The signature-based approaches monitor the system and compare it with pre-defined abnormal patterns [10]. As the performance of the signature-based approach greatly relies on the quality and amount of these pre-defined abnormal patterns, it has to maintain a comprehensive and up-to-date anomaly dictionary. Therefore, it is not suitable for the detection of time-sensitive systems like UAVs, especially considering its restricted onboard computing resources.

The redundancy-based approaches [11]–[13] typically deploy redundant hardware and software components to perform cross-check of their status at runtime. Although these redundant components are only used for critical system tasks, they inevitably cause additional cost and system complexity. For example, multiple versions of the same controllers have to be implemented to enable some redundancy-based approaches. In addition, the redundant-based approaches cannot handle abnormal status caused by the defects of UAV parts (e.g., a crack on the propeller), since the duplication of these parts is physically impractical.

The behavioral-based approaches [14]–[17] describe the normal system operations using a specification. In the specification, constraints are usually programmed in terms of the program state or execution time of specific operations. The behavioral-based approaches mainly focus on program-level anomalies, in which behaviors in the system are considered abnormal if these specified constraints are not met. However, the abnormal status of a UAV system can be caused by many factors without touching the program-level.

The learning-based approaches have received many research efforts in recent years [18]–[22] with the rapid development of machine learning/deep learning algorithms and hardware. For example, Nvidia's Jetson AI modules [23] have been adopted by multiple UAV platforms to support machine learning and AI operations. The learning-based approach monitors the status of a system using a trained machine learning or deep learning model. The main challenge in learning-based approaches is how to obtain a high-quality data set with sufficient normal and abnormal records for training, especially for the abnormal data. Unsupervised learning has the potential to eliminate the need for abnormal data, nevertheless, it can be susceptible to a high false positive rate. In this paper, we overcome this challenge by leveraging our UAV cybersecurity simulation platform to simulate different flying conditions with the injection of anomalies caused by different factors.

III. Detailed Construction

The construction of our detection system consists of three major stages as presented in Fig.1: (1) the collection of IMU sensor data from UAV operations under both normal and abnormal status; (2) the selection, training, and tuning of appropriate DNN models for UAV anomaly detection; (3) the construction of the detection system based on the DNN model. In the following, we present the details of each stage in our construction.

A. Data Collection and Labeling

A high-quality data set is an essential component of training deep learning models and help them perform the desired task. Therefore, the first task in our construction is to collect a balanced data set that contains sufficient IMU sensor data from both normal and abnormal operations of UAVs. While the normal data can be quickly collected by flying UAVs regularly, the generation of sufficient abnormal data faces challenges from the following two aspects: (1) the appearance of abnormal operation status of UAVs in field tests can cause the crash of UAVs and lead to high experimental cost due to hardware replacement; (2) a high-quality data set needs to cover data from abnormal status under different conditions,

which include the variation of abnormal status in terms of UAV models, strength, duration, frequency, patterns, as well as IMU parameters. To overcome these challenges, we leverage our UAV cybersecurity simulation platform [24] to simulate the operation of UAVs under different abnormal status. In particular, PX4 Autopilot [25], Gazebo [26], and QGround-Control [27] are adopted to establish the flying environment of UAVs with different UAV models. We then develop the cybersecurity plug-ins and integrate them into the simulation platform, which will trigger the corresponding abnormal status of UAVs during operations. As an example shown in Fig.2, we can customize UAV flying plans that cover both normal and abnormal UAV status to support the data collection of the training of DNN models. An example of the corresponding IMU sensor data samples on x-acceleration with regard to the abnormal UAV status is presented in Fig.3. To collect sufficient data for training, we simulate different flying plans with 7 hours of flying, which consists of both normal flying plans and flying plans with different anomalies injected.

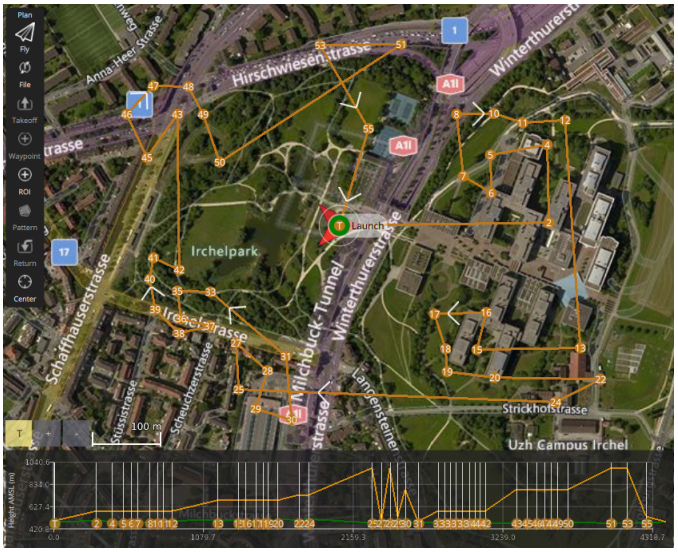

Fig. 2. Example of a Flying Plan

To prepare the data set for training, we apply different time windows on the time series data we collected in the simulation. We vary the duration of time windows from 0.5 second to 5 seconds on the collected data, and represent each time window as a data vector. A longer time window contains more data points, however, will also lead to a longer data collection time for the UAV to perform real-time monitoring and detection. When labeling the collected time windows, we consider a time window as abnormal when $T\%$ of its data points are abnormal. Hence, the value of T can be used as the threshold and adjusted to optimize the detection accuracy. When the value of T is too small, it may cause a high false positive rate since a small number of abnormal data points can also be introduced by environmental factors, such as UAV vibration caused by wind. Likewise, a large T can lead to the miss of detection for short abnormal status that does not contain

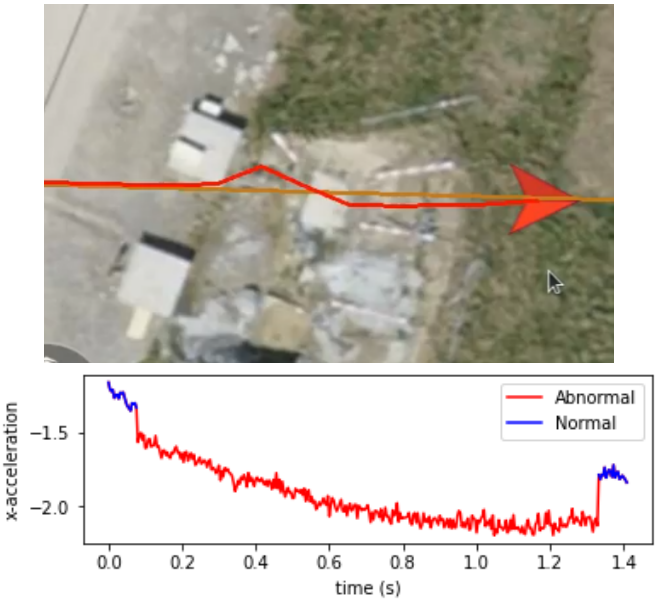

Fig. 3. Example of Abnormal Status in the Flying and the Abnormal IMU Sensor Data Samples on x-acceleration

sufficient abnormal data points. According to our evaluation results, we set time window as 0.5-second and $T\% = 40\%$ in our construction. More detailed analyses are provided in Section IV-A.

B. DNN Model Selection and Training

To identify an appropriate DNN model to build the abnormal detection system for the UAV, we examined major architectures that have been demonstrated to be effective when handling time series data, including CNN, unidirectional long short-term memory (LSTM) [28], bidirectional LSTM (BiLSTM), as well as the combination of CNN and LSTM. In particular, we consider two combinations of CNN and LSTM: (1) CNN is used to extract features from raw data and then feed them into the LSTM for sequence prediction (CNN+LSTM), and (2) directly integrated CNN into LSTM (ConvLSTM). We consider CNN and LSTM architectures because CNN has been demonstrated to be effective for anomaly detection in different systems [29]. In addition, LSTM is capable of learning the relationship between past data values and current data values and representing that relationship in the form of learned weights, which further preserve the features in the time-series data.

After evaluating different DNN models, our construction adopts and tunes the CNN model as presented in Fig.4. Specifically, convolutional layers are utilized as feature extractors and a dropout layer is applied after them to prevent the network from overfitting. After that, the pooling layer is used to reduce the number of parameters in the model prior to classification. The outputs are then flattened and fed into the fully-connected layer with an output size of 2 for final classification with the follow-up softmax layer and a classification layer. Our CNN model achieves the best detection accuracy, especially

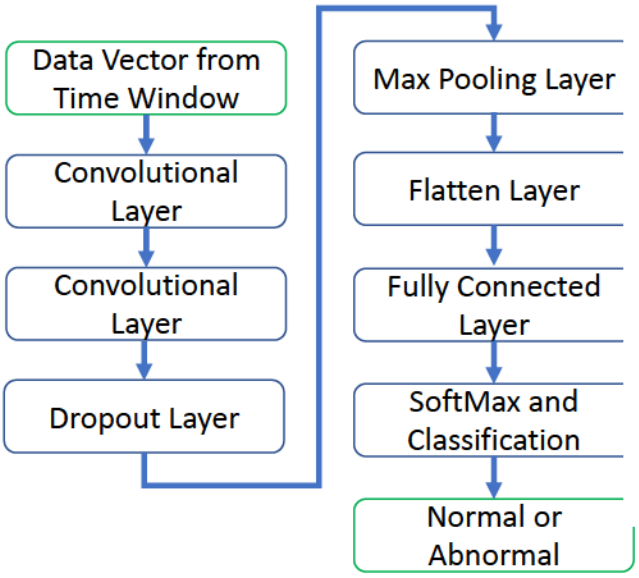

Fig. 4. Architecture of Adopted CNN Model

when short time windows are adopted to enable fast detection. The evaluation and comparison results between different DNN models are detailed in Section IV-A.

C. Construction of Detection System

Based on the CNN model, we now construct the anomaly detection system as shown in Fig.5. The UAV system has the pre-trained CNN model deployed on it. To perform real-time anomaly detection, the UAV keeps monitoring the IMU sensor data and processing it according to the time window adopted by the pre-trained CNN model. By feeding the processed IMU sensor data into the CNN model, it outputs whether the data is abnormal or not. To reduce the false positive rate during the detection, our system considers a two-level abnormal determination, i.e., high-level warning if the probability of the monitored data to be abnormal is greater than 65%, otherwise low-level warning. If a high-level warning is detected, our system will warn the UAV system immediately to trigger its protection strategies (e.g., UAV safe mode). For a low-level warning, our system will perform a secondary check, which will turn the low-level warning to high-level if another low-level warning is detected in the next five time windows.

IV. Evaluation

In this section, we present our evaluation of the proposed anomaly detection system. Receiver operating characteristic curve (ROC curve) [30] is used to measure the accuracy of our detection system with the true positive rate (TPR) and false positive rate (FRP), because the detection system can be mapped as a classification problem with two categories, i.e., normal and abnormal. $TPR = \frac{TP}{TP+FN}$ measures the capability of our detection system to correctly identify abnormal data and $FPR = \frac{FP}{FP+TN}$ measures the errors made by our detection system that classify normal data as

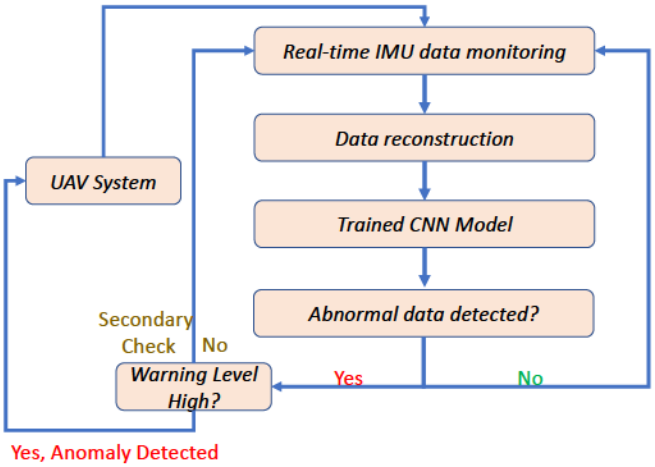

Fig. 5. UAV Anomaly Detection System

abnormal, where FN and TN denote false negative and true negative respectively. Therefore, we aim to increase the TPR of our proposed detection system while lowering its FPR, which is measured by the Area under the ROC Curve (AUC) [30]. AUC measures how well the detection model is capable of distinguishing between classes, and a higher AUC value ($0 \sim 1$) indicates a better performance of the detection model, in which AUC = 0 and AUC = 1 indicate the 0% and 100% accuracy respectively.

A. Evaluation Results

In our evaluation, we performed extensive experiments to explore the impact of different factors on the performance of our proposed detection system, including the selection of DNN models, the duration of time windows for detection, and the threshold value T. In addition, our evaluation considers different types of abnormal status to validate the performance of our detection system.

Fig. 6. Evaluation Results on Different DNN models

We first evaluate the performance of different DNN models in our detection system. We trained and tested 6 different CNN and LSTM-based DNN models. All models are trained with 200 epochs. As shown in Fig.6, CNN-based detection system achieves the best performance for the detection of UAV abnormal status with AUC = 0.82. It is also notable that models with CNN layers involved achieve a better performance than these LSTM-only models. Therefore, CNN is adopted in the construction of our detection system.

To determine the appropriate time window used for the detection of abnormal status, we vary it from 0.5 second to 5 seconds for our CNN-based detection system as presented in Fig.7. Although the best detection performance can be achieved by the 5-second time window with AUC = 0.921, it also significantly increases the real-time data collection time for each detection. As anomaly detection is a time-sensitive task for UAVs, earlier detection of abnormal status is important to protect the UAV against potential security threats and hardware/software failures. Therefore, our detection system adopts the 0.5-second time window that achieves AUC = 0.826. With regard to the threshold value $T\%$ in our construction, we vary it from 0% to 50% as shown in Fig.8. $T\% = 20\%$ is adopted in our construction since it achieves the best accuracy with $AUC = 0.871$ and a relatively lower threshold will also increase the sensitivity of our detection model towards abnormal status of UAVs.

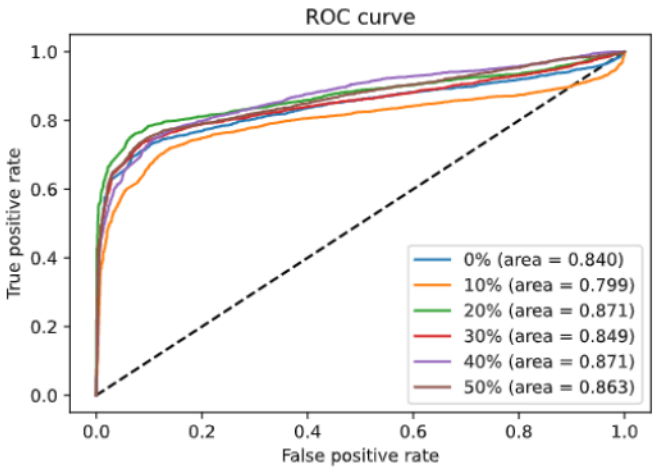

Fig. 8. Evaluation Results on Different Threshold Values

detect anomalies with different duration and achieves a stable performance with AUC from 0.841 to 0.881

Fig. 7. Evaluation Results on Different Time Windows

We now evaluate the performance of our detection system for different anomalies. We first consider anomalies that affect different components of the IMU, including accelerometer only, accelerometer+gyroscope, and accelerometer+gyroscope+orientation. As shown in Fig.9, our detection system achieves the best performance (AUC = 0.937) for anomalies that only affect the accelerometer, and is also effective for other types of anomalies that affect multiple components in the IMU. Moreover, we also evaluate anomalies with different duration, from $1 \sim 2$ seconds to $4 \sim 5$ seconds. Fig.10 shows that our detection system is effective to

Fig. 9. Evaluation Results on Different Types of Anomalies

V. Conclusion and Future Work

In this paper, we propose a UAV anomaly detection system powered by the CNN-based IMU sensor data analysis. By examining and analyzing different DNN models and detection time windows in our design, we optimize to balance the performance of our detection system in terms of accuracy and efficiency. A data set for UAV IMU data is collected and labeled with our extensive simulation using our UAV cybersecurity platform, which not only supports the training of CNN models in our design, but will also benefit the other related research in the community (e.g., IMU-based UAV tracking). Our evaluation results demonstrate that our detection system achieves high accuracy under different conditions.

As future work, we plan to further test and evaluate our proposed detection system using hardware-in-the-loop simu-

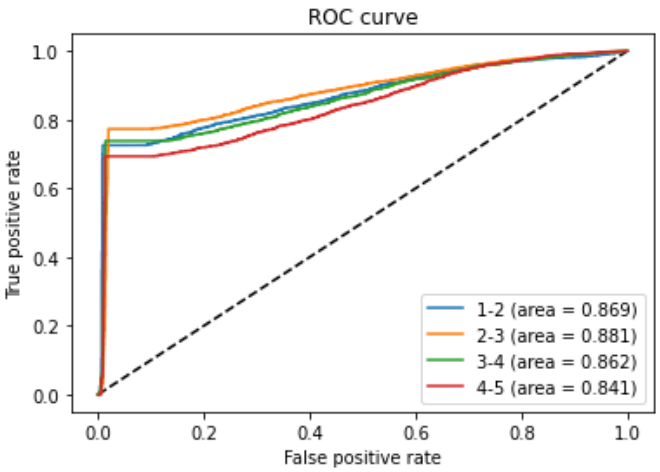

Fig. 10. Evaluation results on Anomalies with Different Duration

lation and field tests. In addition, we plan to design a fail-safe mechanism for UAVs to protect them from detected anomalies.

ACKNOWLEDGMENTS

This work is supported by the US National Science Foundation awards (CNS-2050972 and DGE-1956193) and UMass Dartmouth Cybersecurity Center Fellowship.

REFERENCES

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

[2] 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.

[3] 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.

[4] 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.

[5] Federal Aviation Administration. UAS by the Numbers. https://www.phillybyair.com/blog/drone-stats/, 2021.

[6] C. G. L. Krishna and R. R. Murphy. A review on cybersecurity vulnerabilities for unmanned aerial vehicles. In *2017 IEEE International Symposium on Safety, Security and Rescue Robotics (SSRR)*, pages 194–199, Oct 2017.

[7] Zhongli Liu, Zupei Li, Benyuan Liu, Xinwen Fu, Ioannis Raptis, and Kui Ren. Rise of mini-drones: Applications and issues. In *Proceedings of the 2015 Workshop on Privacy-Aware Mobile Computing*, PAMCO '15, page 7–12, New York, NY, USA, 2015. Association for Computing Machinery.

[8] Hongjun Choi, Wen-Chuan Lee, Yousra Aafer, Fan Fei, Zhan Tu, Xiangyu Zhang, Dongyan Xu, and Xinyan Deng. Detecting attacks against robotic vehicles: A control invariant approach. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, CCS '18, page 801–816, New York, NY, USA, 2018. Association for Computing Machinery.

[9] Yunmok Son, Hocheol Shin, Dongkwan Kim, Youngseok Park, Juhwan Noh, Kibum Choi, Jungwoo Choi, and Yongdae Kim. Rocking drones with intentional sound noise on gyroscopic sensors. In *24th USENIX Security Symposium (USENIX Security 15)*, pages 881–896, Washington, D.C., August 2015. USENIX Association.

[10] Sanmeet Kaur and Maninder Singh. Automatic attack signature generation systems: A review. *IEEE Security Privacy*, 11(6):54–61, 2013.

[11] Man-Ki Yoon, Sibin Mohan, Jaesik Choi, Jung-Eun Kim, and Lui Sha. Securecore: A multicore-based intrusion detection architecture for real-time embedded systems. In *2013 IEEE 19th Real-Time and Embedded Technology and Applications Symposium (RTAS)*, pages 21–32, 2013.

[12] Man-Ki Yoon, Bo Liu, Naira Hovakimyan, and Lui Sha. Virtualdrone: Virtual sensing, actuation, and communication for attack-resilient unmanned aerial systems. In *2017 ACM/IEEE 8th International Conference on Cyber-Physical Systems (ICCPS)*, pages 143–154, 2017.

[13] Fan Fei, Zhan Tu, Ruikun Yu, Taegyu Kim, Xiangyu Zhang, Dongyan Xu, and Xinyan Deng. Cross-layer retrofitting of uavs against cyber-physical attacks. In *2018 IEEE International Conference on Robotics and Automation (ICRA)*, pages 550–557, 2018.

[14] Christopher Zimmer, Balasubramanya Bhat, Frank Mueller, and Sibin Mohan. Time-based intrusion detection in cyber-physical systems. In *Proceedings of the 1st ACM/IEEE International Conference on Cyber-Physical Systems*, ICCPS '10, page 109–118, New York, NY, USA, 2010. Association for Computing Machinery.

[15] Stanley Bak, Karthik Manamcheri, Sayan Mitra, and Marco Caccamo. Sandboxing controllers for cyber-physical systems. In *2011 IEEE/ACM Second International Conference on Cyber-Physical Systems*, pages 3–12, 2011.

[16] Robert Mitchell and Ing-Ray Chen. Adaptive intrusion detection of malicious unmanned air vehicles using behavior rule specifications. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 44(5):593–604, 2014.

[17] Robert Mitchell and Ing-Ray Chen. Behavior rule specification-based intrusion detection for safety critical medical cyber physical systems. *IEEE Transactions on Dependable and Secure Computing*, 12(1):16–30, 2015.

[18] Alireza Abbaspour, Kang K. Yen, Shirin Noei, and Arman Sargolzaei. Detection of fault data injection attack on uav using adaptive neural network. *Procedia Computer Science*, 95:193–200, 2016. Complex Adaptive Systems Los Angeles, CA November 2-4, 2016.

[19] Yuqi Chen, Christopher M. Poskitt, and Jun Sun. Learning from mutants: Using code mutation to learn and monitor invariants of a cyber-physical system. In *2018 IEEE Symposium on Security and Privacy (SP)*, pages 648–660, 2018.

[20] Khurum Nazir Junejo and Jonathan Goh. Behaviour-based attack detection and classification in cyber physical systems using machine learning. In *Proceedings of the 2nd ACM International Workshop on Cyber-Physical System Security*, CPSS '16, page 34–43, New York, NY, USA, 2016. Association for Computing Machinery.

[21] Benkuan Wang, Zeyang Wang, Liansheng Liu, Datong Liu, and Xiyuan Peng. Data-driven anomaly detection for uav sensor data based on deep learning prediction model. In *2019 Prognostics and System Health Management Conference (PHM-Paris)*, pages 286–290, 2019.

[22] Dawei Pan, Longqiang Nie, Weixin Kang, and Zhe Song. Uav anomaly detection using active learning and improved s3vm model. In *2020 International Conference on Sensing, Measurement Data Analytics in the era of Artificial Intelligence (ICSMD)*, pages 253–258, 2020.

[23] Nvidia Jetson Solutions for Drones & UAVs. https://www.nvidia.com/pt-br/autonomous-machines/uavs-drones-technology/.

[24] Ashok Raja, Julio Galvan, Yanyan Li, and Jiawei Yuan. Uclp: A novel uav cybersecurity laboratory platform. In *ACM Annual Conference on IT Education (SIGITE)*, 2021.

[25] PX4 Autopilot. https://px4.io/.

[26] Gazebo Simulator. http://gazebosim.org/.

[27] QGroundControl. http://qgroundcontrol.com/.

[28] Sepp Hochreiter and Jürgen Schmidhuber. Long short-term memory. *Neural Comput.*, 9(8):1735–1780, November 1997.

[29] Montdher Alabadi and Yuksel Celik. Anomaly detection for cyber-security based on convolution neural network : A survey. In *2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, pages 1–14, 2020.

[30] Tom Fawcett. An introduction to roc analysis. *Pattern Recognition Letters*, 27(8):861–874, 2006. ROC Analysis in Pattern Recognition.