Secured UAV Navigation: A Novel Intrusion Detection System Based on PWM Signal Analysis

Alvaro Alva*, Luis Martinez Moreno*, Muneeba Asif*, Alvi Ataur Khalil*,
Mohammad Ashiqur Rahman*, Alfredo Cuzzocrea†, and Shahriar Hossain‡
*Department of Electrical and Computer Engineering, Florida International University, USA
†University of Calabria, Rende, Italy ‡University of West Florida, USA
{aalva513, lmart549, masif004, akhal042, marahman}@fiu.edu,
alfredo.cuzzocrea@unical.it, hshahria@kennesaw.edu

***Abstract*—Unmanned Aerial Vehicles (UAVs) have seen exponential growth in applications, from surveillance to logistics. Ensuring their security, especially in a Global Position System (GPS)-compromised environment, is critical. This paper introduces an Intrusion Detection System (IDS) as a countermeasure against sensor's attacks that leverages Pulse Width Modulation (PWM) signals, generated by the UAV Board. The IDS, positioned at the Electronic Speed Controllers (ESCs), can potentially detect anomalies even when conventional ground station detections fail. Multiple unsupervised machine learning algorithms were evaluated for this purpose. The Local Factor Outlier (LOF) emerged as the most accurate with 75.87%, closely followed by One Class SVM (OCSVM) at 74.17%, and Isolation Forest (IF) at 71.59%. These findings suggest that monitoring PWM signals could provide a novel layer of security for UAVs, making them resilient against certain forms of cyber-attacks.**

***Index Terms*—PWM, ESC, UAV, IDS, One-Class SVM, Isolation Forest, Local Outlier Factor**

I. Introduction

Unmanned Aerial Vehicles (UAVs), often referred to as drones, have seen remarkable advancements in recent years. These sophisticated machines are rapidly integrating into various sectors such as agriculture, communications, surveillance, and transportation [1]–[5]. However, with the increased integration and reliance on these UAVs, security has become a paramount concern. Recent studies have delved into the detection of cyber threats targeting these aerial vehicles [6]–[8]. From eavesdropping attacks to data injection threats, the vulnerabilities in UAV-aided systems are numerous. For instance, Gu et al. [9] highlighted the implications of false data injection attacks on UAVs, stressing the importance of establishing robust detection mechanisms.

Machine learning (ML) techniques have been recognized as pivotal in fortifying UAV systems, including regression-based anomaly detection techniques (e.g., [10]). Several researchers have ventured into novel methods for UAV intrusion detection. For instance, Whelan et al. [11] proposed a novelty-based approach to detect sensor attacks on UAVs, while Basan et al. [12] introduced a self-diagnosis method predicated on parameter change analysis. Furthermore, lightweight solutions are in the spotlight [13], [14], with endeavors [15] emphasizing power electronics for UAV intrusion detection.

GPS-centric cyber-attacks, particularly spoofing and jamming, are emerging as palpable threats [16]. Conventional IDSs frequently hinge on the integrity of sensors and the reliability of communication between UAVs and control stations [17], [18]. Our novel approach recognizes the potential weaknesses in these assumptions and introduces an IDS that meticulously analyzes PWM signals from the UAV board. Positioned at the ESCs like it's shown in Fig. 1, this IDS aims to detect malicious interferences by examining PWM anomalies, a strategy that holds promise even when traditional measures falter [19]. Using unsupervised machine learning algorithms, such as the OC-SVM [20], IF, and LOF [21], this research delves deep into the realm of UAV cybersecurity, setting a blueprint for future research endeavors. To the best of our knowledge this is the first work leveraging the PWM signals to secure the navigational systems in UAVs.

Embedded within the UAV board, four distinct PWM signals play a pivotal role in directing the ESCs, which in turn orchestrate the rotations of the four UAV rotors [22]. Despite being under the duress of malevolent attacks like spoofing or jamming, UAVs have showcased remarkable resilience, often maintaining flight without immediate discernible disruptions [23]. This ostensibly seamless operation, however, can obfuscate the underlying adversarial actions, rendering them imperceptible to the human eye but potentially discernible through anomalies in PWM signals. To sum up, sensor data can be corrupted. That's why we rely on PWM signals for the case where UAVs sensors have been compromised, but the UAV is still flying.

Recognizing this unique characteristic of UAVs, our paper elucidates a novel IDS centered on PWM signals. Designed as a formidable defense, this IDS is particularly vital when conventional UAV sensors are potentially compromised or when there's a divergence between the actual sensor data and the data relayed to the control station. Our core contributions are:

- Advocating PWM signals' efficiency in exposing attacks: A comprehensive exploration into how these signals, generated at the flight controller of a UAV, traverse to the ESCs, culminating in the precise maneuvering of UAVs.
- Innovative IDS Framework: A novel IDS rooted in the nuances of PWM signals, further bolstered by unsuper-

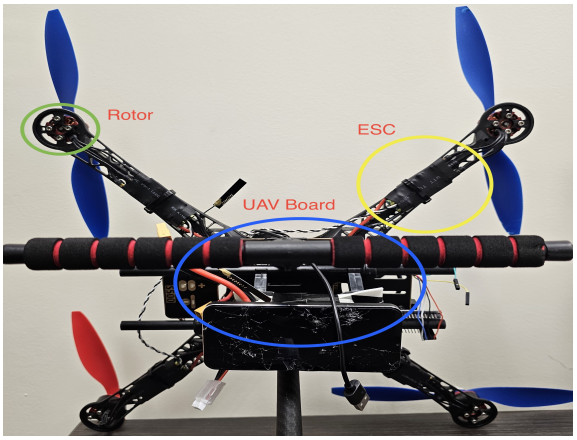


Fig. 1: The Pixhawk PX4 UAV, which is considered in this work. ESC and rotor are highlighted.

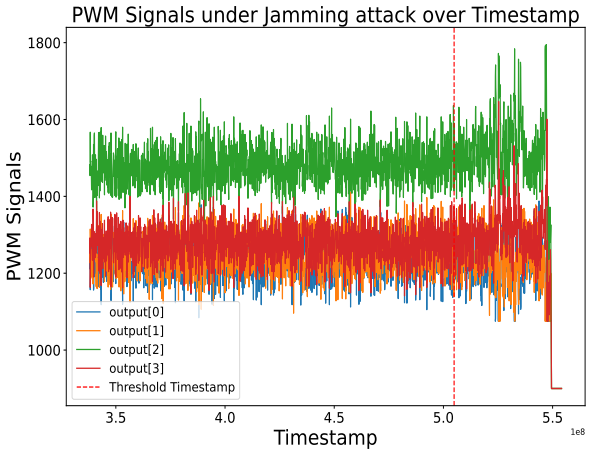


Fig. 2: Illustration of PWM signals over the time. Jamming attack happening after red dotted lines.

vised ML algorithms. The framework is tailored to act when other monitoring systems deliver deceptive data.

- Empirical Analysis: An exhaustive evaluation of the proposed IDS, contextualized against traditional algorithms, highlighting its areas of strength and potential for enhancement.

The representation of the PWM signals over the time can be found on Figure 2 and Figure 3 for the cases under Jamming and Spoofing attack, respectively. The measures after the red dotted lines represents the values of the PWM signals under attack.

The objective is to amalgamate the theoretical intricacies of UAV operations with pragmatic defense mechanisms, thereby fortifying the security paradigm of UAVs in real-world applications. Many related works of UAV attacks, sensor-based IDS, and side-channel analysis will be referenced in section II. The background will be explained in section III. The technical details of this research will be elaborated in section IV. Once all concepts are well defined, in section V the proposed IDS

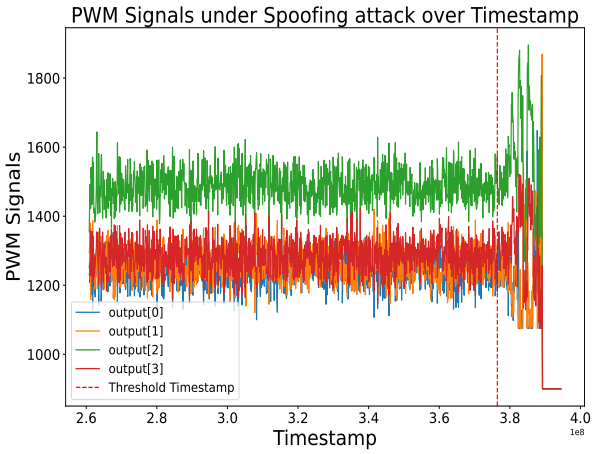


Fig. 3: Illustration of PWM signals over the time. Spoofing attack happening after red dotted lines.

will be shown. Most important metrics will be presented in section VI. Finally, we will conclude the paper with some future directions in section VII.

II. Related Work

The increasing reliance on UAVs across various sectors has necessitated a surge in research dedicated to identifying and addressing their security vulnerabilities. This section will scrutinize key studies that have contributed to understanding UAV security gaps, particularly from the angle of machine learning and PWM signal analysis.

Hoang et al. [20] explored unsupervised learning techniques for eavesdropping attack detection in UAV-aided wireless systems, utilizing OC-SVM and K-Means clustering. Their research, while innovative, does not fully address the nuances and potential false positives inherent in unsupervised learning nor its adaptability to varying attack patterns. The survey by Šimon et al. [24] on using deep learning to combat UAV jamming and deception attacks draws attention to the adaptability of neural networks. However, the study could benefit from a deeper analysis of how these models perform under active adversarial conditions and the implications of model interpretability in real-world scenarios. Yang et al. [25] proposed a hybrid model combining CNN-2D, CNN-1D, RF, and SVM to predict landslides. Although they reported an accuracy of 82.79%, their model's reliance on high-quality, correlated input data may not be realistic in all UAV operational environments, where data can be noisy or incomplete.

In the realm of side-channel analysis, Yu et al. [6] and Lerman et al. [26] demonstrated the utility of machine learning to exploit UAV system vulnerabilities through side-channel signals. However, the specificity of such attacks and the need for sophisticated equipment can limit the practicality of these approaches. Radtke et al. in [27] proposed a UAV's safeguard against side-channel analysis through Motor Noise Injection

(MNI), but its robustness in real-world scenarios where environmental noise could interfere with the MNI strategy could be a limitation.

Research in [15] reported potential attacks on a Pixhawk UAV Flight Controller like False Data Injection (FDI) to sensors, Firmware attacks, and Hardware Trojans. As defense, they identified three ways of detection: PWM signals in normal operations, PWM signals under attack, and SVM modeling of PWM signals in both situations. Albeit hypothesized, these ideas were not thoroughly investigated.

Our work seeks to address these gaps by introducing an unsupervised IDS that scrutinizes PWM signals to identify potential security breaches, offering a novel perspective in the UAV security landscape.

III. Background

To grasp the intricacies of the proposed IDS premised on PWM signals, it's crucial to delve into the foundational aspects of UAV operations and their associated vulnerabilities.

A. PWM generation at UAV Board

Every UAV has a main board that receives all data from sensors, send that data to the Ground Control Station (GCS), and moves the rotors according to the PWM signals created from the response of the GCS back to the main board. For this research project, we are using the Pixhawk 2.8 flight controller, represented in Fig. 1, as the main board with four sensors: gyroscope, GPS/compass, barometer, and accelerometer accordingly to the Pixhawk documentation in [22]. PWM signals have long been an integral component of various electronic systems, owing to their ability to control the amount of power delivered to a device without wasting energy. In the context of UAVs, these signals have a pivotal role in maneuvering and navigation.

Generation and functionality: UAVs, particularly those equipped with the Pixhawk board, generate the number of rotors as well as distinct PWM signals. For this project the UAV has 4 rotors therefore 4 PWM signals. These signals are represented in Fig. 4 with names "output[0]", "output[1]", "output[2]", and "output[3]". These signals are directed towards the ESCs, which, in turn, dictate the rotations of the UAVs four rotors. It's this intricate dance of PWM signals that ensures the UAVs precise movements and stability during flight.

B. GPS Navigation on UAVs

GPS forms the backbone of most modern UAV navigation systems. By triangulating signals from multiple satellites, UAVs can determine their precise position and altitude, ensuring accurate navigation and stable flight.

Susceptibility to attacks: While GPS provides invaluable spatial information, it is also vulnerable to adversarial interventions. Spoofing attacks, wherein false signals are broadcasted to mislead the GPS receiver, or jamming attacks that block the GPS signals entirely, pose significant threats to UAV operations. In Figure 4, we have shown the no correlation between the most representative features of a sensor-based IDS and PWM signals. Any value between [-0.3,0.3] represents low or null correlation.

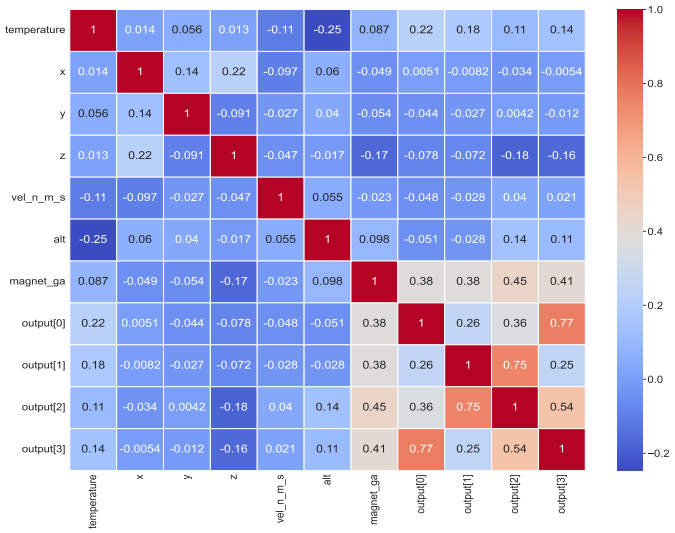


Fig. 4: Correlation heatmap of PWM signals vs Sensors features.

C. Why UAVs can be Secured on PWM-based IDS?

UAVs, with their increasing ubiquity and diverse applications, are not just technological marvels but also represent points of vulnerability in the digital ecosystem. Traditional IDS for UAVs use mostly sensors data that are processed at the UAV board and send to the GCS via wireless communication. Those 2 Open Systems Interconnection (OSI) layers are susceptible for attacks like spoofing, at the Data Link layer, and jamming, at the Transport layer. Therefore, an IDS located at the ESCs, which belongs to the Physical layer, can alert the UAV if it's under attack.

As underscored earlier, adversarial interventions may not immediately disrupt a UAV's flight. A UAV under attack might still seem to operate smoothly, masking the underlying intrusion to an untrained observer. This underscores the need for layered defense mechanisms that can detect and mitigate threats even when primary sensors or communication channels might be compromised.

IV. Technical Details

This section elaborates on the foundational assumptions of our threat model, outlines the potential adversary knowledge spectrum, and explicates the objectives and ramifications of their attacks.

A. Assumptions

We consider the following assumptions:

- GPS as a Primary Target: We recognize that adversaries primarily target the UAV's GPS system for exploitation through spoofing or jamming. The objective of these attacks is to mislead or disrupt the UAV's navigational capabilities.

- Sophisticated Adversaries: Assumed attackers possess high-level technological expertise, enabling them to craft refined GPS-based attacks without causing immediate or overt disruptions in the UAV's flight.
- External Attacks: The threat model is centered on external adversaries. These individuals or entities lack physical access to the UAV but can tamper with its communication channels, particularly the signals pertaining to the GPS system.

B. Knowledge of the Attacker

There are many channels a UAV can be susceptible from an attack. Abro et al. in [28] detail how the sensors and communication channels could been hacked by an attacker. There is no attack directly to the PWM signals yet as of our knowledge. That's why we are relying on them. We can summarize that the attacker might have the following knowledge:

- Partial Knowledge: Such adversaries are aware of general UAV operations and the centrality of the GPS in its navigation.
- Advanced Knowledge: A subset of attackers might harbor deeper insights, such as specifics about the UAVs GPS communication protocols or potential vulnerabilities therein, or even could compromise the firmware to spoof the data coming from the Data Link layer to the Application layer.

C. Attack Goal

The attacker has the following goals:

- Trajectory Deviation: An intricate form of attack where counterfeit GPS signals are broadcasted, aiming to mislead the UAV's GPS receiver and divert it from its designated path.
- Denial of Service: A more direct form of assault wherein adversaries emit powerful interference signals to entirely obstruct the UAVs GPS communication, rendering its navigational system ineffective.

D. Attack Impact

The consecuences of the attack can be:

- Deceptive Normalcy: A UAV under a spoofing or jamming attack could, to an untrained observer or basic sensors, seem to operate normally. This deceptive appearance makes the attacks even more threatening as they can persist undetected.
- Operational Deviations: Over time, even subtle GPS tampering can lead to significant deviations in the UAV' operations, from its path to its task execution.
- Compromised Sensor Data: Given that these attacks target the GPS, the data from the GPS sensors can be misleading. If these compromised data are trusted by the GCS, it could lead to flawed decision-making.

Considering the above impacts and the potential for compromised primary sensors, there arises a critical need for an auxiliary detection mechanism. This is the crux behind deploying an IDS at the ESCs level. By monitoring PWM signals, which are inherently influenced by the UAV's operations (and indirectly by its GPS navigation), one can detect the anomalies indicative of GPS-targeted attacks. This IDS acts as a safeguard, stepping in when primary detection methods might be blinded or deceived.

TABLE I: Number of samples.

	Jamming	**Spoofing**	**Total**
Benign	1668	1156	2824
Malicious	493	181	674
Total	2161	1337	3498

V. Proposed IDS

In the rapidly evolving UAV landscape, security has emerged as a primary concern, particularly given the vulnerabilities associated with UAV navigational systems. Recognizing the limitations of traditional sensor-based IDS, especially when those very sensors (like GPS) can be compromised, we present an innovative IDS. This IDS is premised on monitoring PWM signals, acting as a secondary line of defense against navigational anomalies. Here, we delve into the technical intricacies of the proposed IDS, discussing its architecture, the data it utilizes, and its underpinning ML mechanics.

Where PWM signals are generated? Understanding the genesis of PWM signals is fundamental to our IDS's operational paradigm. Within the UAVs structure, specifically the Pixhawk board, four distinct PWM signals are generated. These signals play a pivotal role, interfacing with the ESCs to command the rotations of the UAVs four rotors, thereby ensuring agile and stable flight. Given the direct influence of GPS navigation on the UAVs movements, any GPS-targeted attack will inevitably manifest as deviations in these PWM signals, not visualizable by the human eye. Besides the PWM signals are not correlated with most sensor features like in Fig. 4, it can detect navigational anomalies. There is the novelty.

A. Dataset

High-quality data is the bedrock of any ML-driven system. For this experiment, we have user Hardware-in-the-loop simulation. It consists on operating a simulation on a computer, but having the flight controller and its sensors connected as well. The experimental UAV as shown in 1 have 4 'wings'. Therefore, the simulated UAV flight has output 4 PWM signals due the 4 rotors our UAV has. The maximum number of PWM signals and rotors that the flight controller can support is 16. The minimum is 4. Each PWM signal represents the percentage of time that the digital square-wave of a rotor is within a specific period. The default minimum value for PWM signals is 900 and the maximum is 2000. For our IDS:

- Source: The dataset encapsulates PWM signals captured during regular UAV flights, representing benign scenarios, and patterns observed under conditions where GPS-based attacks, like spoofing or jamming, were simulated. As shown in Table I, we have 3498 samples, from which

2824 samples belongs to benign cases and 674 to malicious cases.

- Features: The dataset houses four primary features, each corresponding to the PWM signals relayed to each of the UAV's rotors. In Fig. 4 we've shown that PWM signals are not correlated with sensor data, and even the correlated between the PWM signals themselves is not too high.

B. Data Pre-processing

Data pre-processing forms the foundational step in enhancing the quality of data before it is fed into any IDS. In the context of UAVs, ensuring clean and reliable data is paramount, given the dynamic and often unpredictable nature of their operational environments.

- Remove Constant Values: Constant values in datasets do not contribute any meaningful information, especially when modeling patterns or anomalies.
- Remove Duplicate Values: By removing such redundant entries, the dataset retains only unique records, ensuring the learning model is not biased and stays generalizable.
- Interpolation: Using a combination of linear and polynomial interpolations, gaps in the dataset were filled, thereby ensuring continuity and completeness of the records.
- Data Split: The pre-processed data was divided into training (80%) and testing (20%) sets, allowing the model to learn from one data subset and be validated against another.

C. Data Normalization

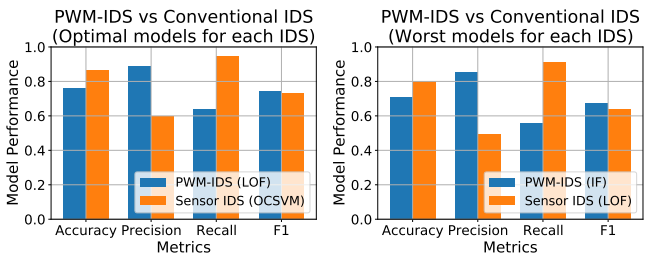
The data obtained from the flight logs has different scale of the features. It is required to apply data normalization to change the values of numeric columns in the dataset to a common scale, without distorting differences in the ranges of values or losing meaningful information for the predictive model. The method we are using is Min-Max Scaling which scales the data to fit within the range of [0,1], where the minimum value of a feature becomes 0 and the maximum value becomes 1.

D. Predictive Model

The purpose of the IDS is to constantly learn from data that has not been under attack. After we have done our pre-processing and normalization steps, we developed the predictive model comparing three unsupervised machine learning algorithms, each offering a distinct lens to view PWM signal anomalies:

One-Class SVM: This high-dimensional data specialist projects the PWM signal patterns into a higher-dimensional space. Once transposed, it aims to demarcate a hyperplane that distinctly separates benign signals from potential anomalies, providing a robust method for detecting subtle adversarial interventions.

Isolation Forest: Harnessing a tree-based strategy, the IF algorithm partitions the dataset using randomly selected attributes. Through this, it assigns anomaly scores rooted in the tree depth. Patterns resulting in shorter tree paths are flagged as probable anomalies, making this approach particularly adept at early-stage intrusion detection.



(a) (b)

Fig. 5: Contrasting the PWM-IDS with conventional sensor data-based IDS with, (a) the best models for each IDS, and (b) with worst models for each IDS.

Local Outlier Factor: Grounded in density-based clustering, LOF computes scores reflecting PWM signals' anomaly levels concerning their immediate neighbors. In doing so, it identifies potential anomalies by discerning local density deviations, capturing both subtle and glaring disruptions.

The results of each algorithm were fine-tuned with different hyper-parameters referred on Table I for optimal performance.

VI. Evaluation

IDS is generalizable to detect anomalies. By systematically analyzing its performance under various scenarios, one can ascertain the strengths and potential weaknesses of the proposed IDS. In Table II we have presented all the performance metrics of the 3 ML algorithms we are using for the predictive model and we also tested them with different hyperparameters. In this section, we delve into the evaluation methodology adopted, the research questions driving the assessment, and a preliminary understanding of the outcomes.

A. Research Questions (RQ)

The evaluation is anchored around several pivotal research questions, aimed at understanding the comprehensive capabilities of the IDS:

RQ1. How can the proposed IDS performs under attack?
RQ2. What is the contrast with other channels IDSs?
RQ3. Can the Physical layer data be used to detect attacks in real-time?

B. Evaluation Results

To methodically address the aforementioned research questions, a series of tests were conducted with the following Research Responses (RES):

RES1. Performance Under Attack.

Our study scrutinized the IDS's response to GPS attack simulations, focusing on malicious PWM patterns. We dissected performance using a testing subset specifically designed to reflect these conditions. The results, detailed in Table II, show that the IDS's efficacy varied across different algorithms.

- Detection Efficacy: With the goal of finding the best model for the IDS, we evaluated multiple ML algorithms,

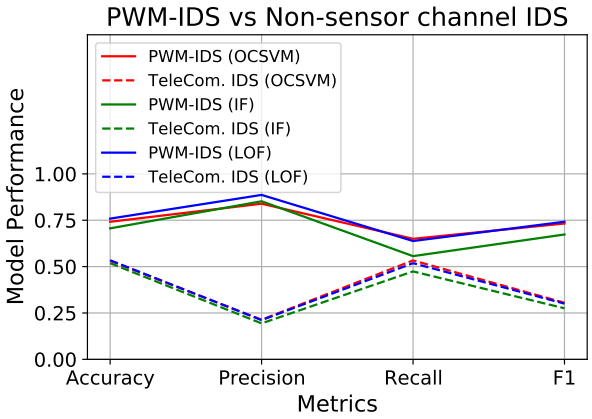


Fig. 6: Contrasting proposed PWM-IDS with another non-sensor channel-based IDS: Telecommunication IDS.

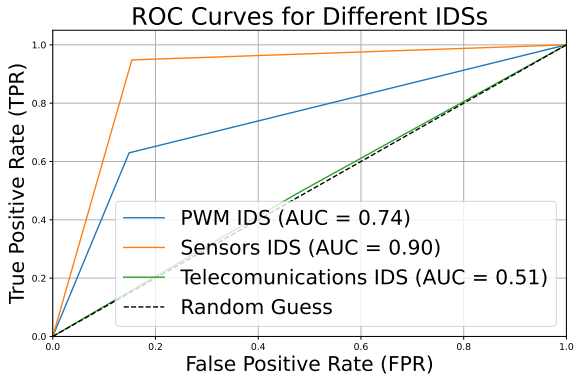


Fig. 7: Comparing the ROC curve and AUC score of the proposed PWM-IDS with different IDSs.

among them the LOF emerged with promise, demonstrating a higher detection rate even when limited to four PWM signals from the UAV's physical layer as the sole features.

- Objective and Accuracy: The primary goal is to hone the most effective model for our IDS. Despite the minimal feature set, the IDS accomplished an accuracy rate of 75.87%, a substantial achievement underlining the potential of our chosen methods.
- Addressing False Positives: We also measured instances where the IDS failed to flag anomalies, known as the False Positive Rate (FPR). For LOF, our leading method, the FPR stood at 9.73%. Given the IDS's limited feature input, this rate is deemed acceptable.
- Continuous Improvement: Moving forward, the objective remains to refine our model, enhancing its precision and reducing false positives. Our efforts are channeled into expanding the feature set and exploring the synergy between them to boost the IDS's defensive capabilities against UAV-related cyber threats.

Due the nature of this simulated experiment, a live UAV flight experiment would precise our metrics obtained by the Hardware-in-the-loop simulation.

RES2. Contrast with other channel IDSs.

We defined what is a sensor-based IDS in the previous sections. Fig. 5 confirms the high reliability of our PWM-based IDS metrics for accuracy, precision, recall, and F1 score with the sensor-based IDS. Nevertheless, a telecommunication-based IDS focuses on the monitoring and analysis of network traffic and communication patterns to detect suspicious activities or intrusions. It operates by inspecting the metadata and content of the packets traveling over the network, looking for signs of known threats like malware signatures, unauthorized data ex-filtration, or attempts to breach the network's defenses.

Our IDS do not require hundreds of features to train, test, or detect in real-time due the PWM signals for most UAVs are just 4. However, the AUC differences over conventional IDSs like in Fig. 7 shows that our IDS actually performs much better than Telecommunication-based IDS and it's getting close to the sensor-based IDS. In addition, the . Lastly, the contrast with a Telecommunication channel IDS even is overperformed by our IDS in Fig. 6. These results prove that an IDS at the Physical layer can be reliable.

RES3. Physical Layer IDS.

While the traditional focus of IDSs has been on network and application layers, the physical layer offers unique challenges, especially for UAVs. The proposed IDS contrasts other channel IDSs by emphasizing the physical layer attributes, such as signal strength, frequency hopping patterns, and physical location discrepancies. Compared to other channel IDSs, the physical layer-based IDS is more adept at detecting spoofing attacks, jamming, and other interference-based intrusions. Furthermore, by using features specific to the physical layer, the proposed IDS avoids the typical overheads associated with inspecting packet contents or higher-level protocol behaviors. This specificity not only streamlines the detection process but also provides granularity in intrusion identification, a facet often lacking in generic IDS solutions.

C. Discussion

The evaluation sheds light on several pivotal insights:

- The choice of unsupervised algorithms, specifically LOF, proves effective for PWM-based intrusion detection, as evidenced by its high detection rates even under sophisticated attacks.
- While the system demonstrates commendable real-time detection capabilities, further optimizations might be explored to enhance its responsiveness, ensuring it remains adept at handling more covert or rapidly evolving threats.

VII. Conclusion

This research proposed an innovative approach to UAV security amidst UAV attacks by focusing on the integrity of PWM signals. Developing an IDS via unsupervised ML algorithms to monitor signals at the ESCs, the paper aimed to ensure the operational stability and security of UAVs, even when sensor data is compromised. Beyond detection, the IDS could be enhanced to make real-time decisions, perhaps triggering countermeasures or alert systems to mitigate potential damage. Research could delve into collaborative defense

TABLE II: Performance comparison of different clustering techniques with varying hyper-parameter values.

Model	Hyperparameter	Accuracy	Precision	Recall	F1
OCSVM	ν=0.010, γ=0.00171	74%	40.01%	70.37%	51.08%
	ν=0.025, γ=0.00332	70.06%	68.36%	83.68%	75.25%
	ν=0.0047, γ=0.00086	74.17%	83.91%	64.99%	73.24%
	ν=0.022, γ=0.00058	73.12%	86.05%	60.39%	70.97%
IF	Contamination=0.27	72.59%	38.65%	71.85%	50.26%
	Contamination=0.43	67.31%	67.78%	78.04%	72.20%
	Contamination=0.12	70.62%	85.22%	55.64%	67.32%
	Contamination=0.19	71.59%	80.38%	63.20%	70.76%
LOF	Neighbors=15, Contamination=0.2	78.29%	45.77%	68.15%	54.76%
	Neighbors=23, Contamination=0.42	70.62%	69.14%	83.09%	75.47%
	Neighbors=11, Contamination=0.09	75.87%	88.66%	63.80%	74.20%
	Neighbors=9, Contamination=0.24	73.77%	76.56%	74.63%	75.58%

mechanisms where a fleet of UAVs work in tandem, sharing threat intelligence and collectively responding to threats. This could be successfully supported by advanced multidimensional visualization paradigms (e.g., [29]).

VIII. Acknowledgment

This research was supported in part by the National Security Agency (NSA) under award H98230-22-1-0327, and the Department of Energy (DOE) under awards DE-CR0000024 and DE-NA0004016. This work was also partially supported by project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU.

References

[1] Alvi Ataur Khalil, Alexander J Byrne, Mohammad Ashiqur Rahman, and Mohammad Hossein Manshaei. Replanner: Efficient uav trajectory-planning using economic reinforcement learning. In *2021 IEEE International Conference on Smart Computing (SMARTCOMP)*, pages 153–160. IEEE, 2021.

[2] Alvi Ataur Khalil, Mohamed Y Selim, and Mohammad Ashiqur Rahman. Cure: Enabling rf energy harvesting using cell-free massive mimo uavs assisted by ris. In *2021 IEEE 46th Conference on Local Computer Networks (LCN)*, pages 533–540. IEEE, 2021.

[3] AHM Jakaria, Mohammad Ashiqur Rahman, Muneeba Asif, Alvi Ataur Khalil, Hisham A Kholidy, Matthew Anderson, and Steven Drager. Trajectory synthesis for a uav swarm based on resilient data collection objectives. *IEEE Transactions on Network and Service Management*, 20(1):138–151, 2022.

[4] Alvi Ataur Khalil and Mohammad Ashiqur Rahman. Fed-up: Federated deep reinforcement learning-based uav path planning against hostile defense system. In *2022 18th International Conference on Network and Service Management (CNSM)*, pages 268–274. IEEE, 2022.

[5] Alvi Ataur Khalil, Mohamed Y Selim, and Mohammad Ashiqur Rahman. Deep learning-based energy harvesting with intelligent deployment of ris-assisted uav-cfmmimos. *Computer Networks*, 229:109784, 2023.

[6] Weize Yu and Yiming Wen. Efficient hybrid side-channel/machine learning attack on XOR PUFs. *Electronics Letters*, (20), October 2019.

[7] 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.

[8] Alvi Ataur Khalil and Mohammad Ashiqur Rahman. Adaptive neuro-fuzzy inference system-based lightweight intrusion detection system for uavs. In *2023 IEEE 48th Conference on Local Computer Networks (LCN)*, pages 1–9. IEEE, 2023.

[9] Yapei Gu, Xiang Yu, Kexin Guo, Jianzhong Qiao, and Lei Guo. Detection, estimation, and compensation of false data injection attack for UAVs. *Information Sciences*, 546:723–741, February 2021.

[10] Rocco Langone et al. Interpretable anomaly prediction: Predicting anomalous behavior in industry 4.0 settings via regularized logistic regression tools. *Data & Knowledge Engineering*, 130:101850, 2020.

[11] Krittika Das et al. Eavesdropping attack detection in uavs using ensemble learning. In *2023 ICEEICT*, pages 01–07, 2023.

[12] Elena Basan, Alexandr Basan, Alexey Nekrasov, Colin Fidge, Ján Gamec, and Mária Gamcová. A Self-Diagnosis Method for Detecting UAV Cyber Attacks Based on Analysis of Parameter Changes. *Sensors*, 21(2):509, January 2021.

[13] Wei-Cheng Hsu. Lightweight CYyberattack Intrusion Detection System for Unmanned Aerial Vehicles Using Recurrent Neural Networks.

[14] Omar Bouhamed et al. Lightweight ids for uav networks: A periodic deep reinforcement learning-based approach. In *2021 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, 2021.

[15] Mohammad Ashiqur Rahman, Md Tauhidur Rahman, Mithat Kisacikoglu, and Kemal Akkaya. Intrusion Detection Systems-Enabled Power Electronics for Unmanned Aerial Vehicles. In *2020 IEEE CyberPELS (CyberPELS)*, pages 1–5, Miami, FL, USA, October 2020. IEEE.

[16] Menaka Pushpa Arthur. Detecting signal spoofing and jamming attacks in uav networks using a lightweight ids. In *2019 CITS*, 2019.

[17] William Koch, Renato Mancuso, Richard West, and Azer Bestavros. Reinforcement Learning for UAV Attitude Control. *ACM Transactions on Cyber-Physical Systems*, 3(2):1–21, April 2019.

[18] Mehran Behjati, Muhammad Aidiel Zulkifley, Haider A. H. Alobaidy, Rosdiadee Nordin, and Nor Fadzilah Abdullah. Reliable Aerial Mobile Communications with RSRP & RSRQ Prediction Models for the Internet of Drones: A Machine Learning Approach. *Sensors*, (15), July 2022.

[19] Xiu-Xiu Ren et al. Protocol-based optimal stealthy data-injection attacks via compromised sensors in cyber-physical systems. *IEEE Transactions on Industrial Electronics*, 2022.

[20] Tiep M. Hoang et al. Detection of Eavesdropping Attack in UAV-Aided Wireless Systems: Unsupervised Learning With One-Class SVM and K-Means Clustering. *IEEE Wireless Communications Letters*, 9, 2020.

[21] Jason Whelan, Thanigajan Sangarapillai, Omar Minawi, Abdulaziz Almehmadi, and Khalil El-Khatib. Novelty-based Intrusion Detection of Sensor Attacks on Unmanned Aerial Vehicles. In *Proceedings of the 16th ACM Symposium on QoS and Security for Wireless and Mobile Networks*, pages 23–28, Alicante Spain, November 2020. ACM.

[22] PX4. Getting to know your devkit, 2023.

[23] Leandro Marcos Da Silva and Fothers. Anomaly-based intrusion detection system for in-flight and network security in uav swarm. In *2023 ICUAS*, pages 812–819, 2023.

[24] Ondřej Šimon and Tomáš Götthans. A Survey on the Use of Deep Learning Techniques for UAV Jamming and Deception. *Electronics*, 11(19):3025, September 2022.

[25] Xin Yang et al. Incorporating landslide spatial information and correlated features among conditioning factors for landslide susceptibility mapping. *Remote Sensing*, 2021.

[26] Liran Lerman et al. Template attacks versus machine learning revisited and the curse of dimensionality in side-channel analysis: extended version. *Journal of Cryptographic Engineering*, 2018.

[27] Timothy Radtke and Cristinel Ababei. Safeguarding unmanned aerial vehicles against side channel analysis via motor noise injection. In *2022 IEEE HOST*, pages 65–68, 2022.

[28] G. Abro et al. Comprehensive review of uav detection, security, and communication advancements to prevent threats. *Drones*, 2022.

[29] Alfredo Cuzzocrea and Svetlana Mansmann. Olap visualization: models, issues, and techniques. In *Encyclopedia of Data Warehousing and Mining, Second Edition*, pages 1439–1446. IGI Global, 2009.