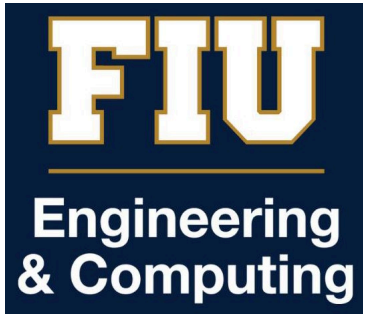


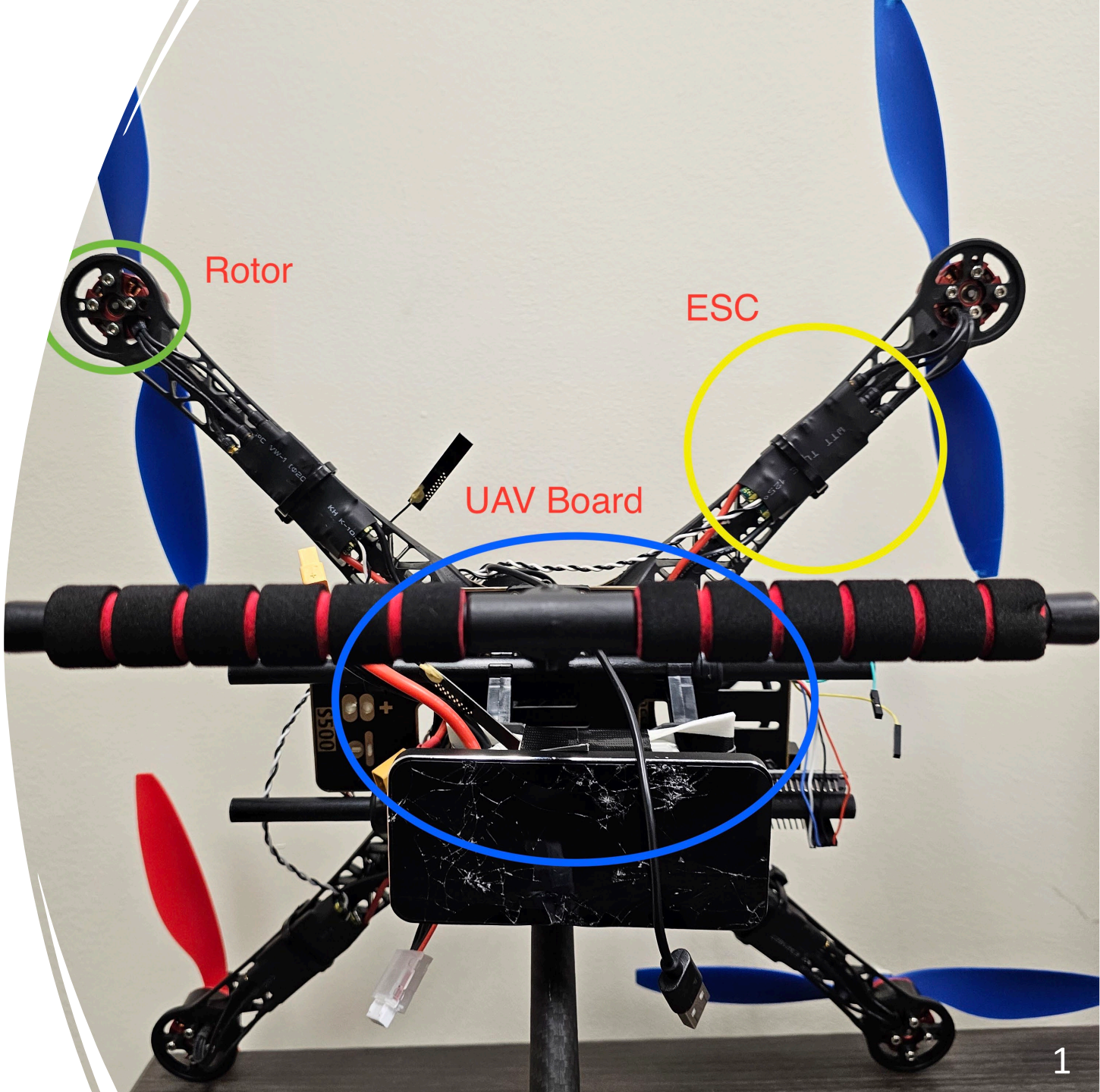
Secured UAV Navigation: A Novel Intrusion Detection System Based on PWM Signal Analysis

Alvaro Alva, Luis Martinez Moreno, Muneeba Asif, Alvi Ataur Khalil, Mohammad Ashiqur Rahman, Alfredo Cuzzocrea, and Shahriar Hossain

Electronic Speed Controler

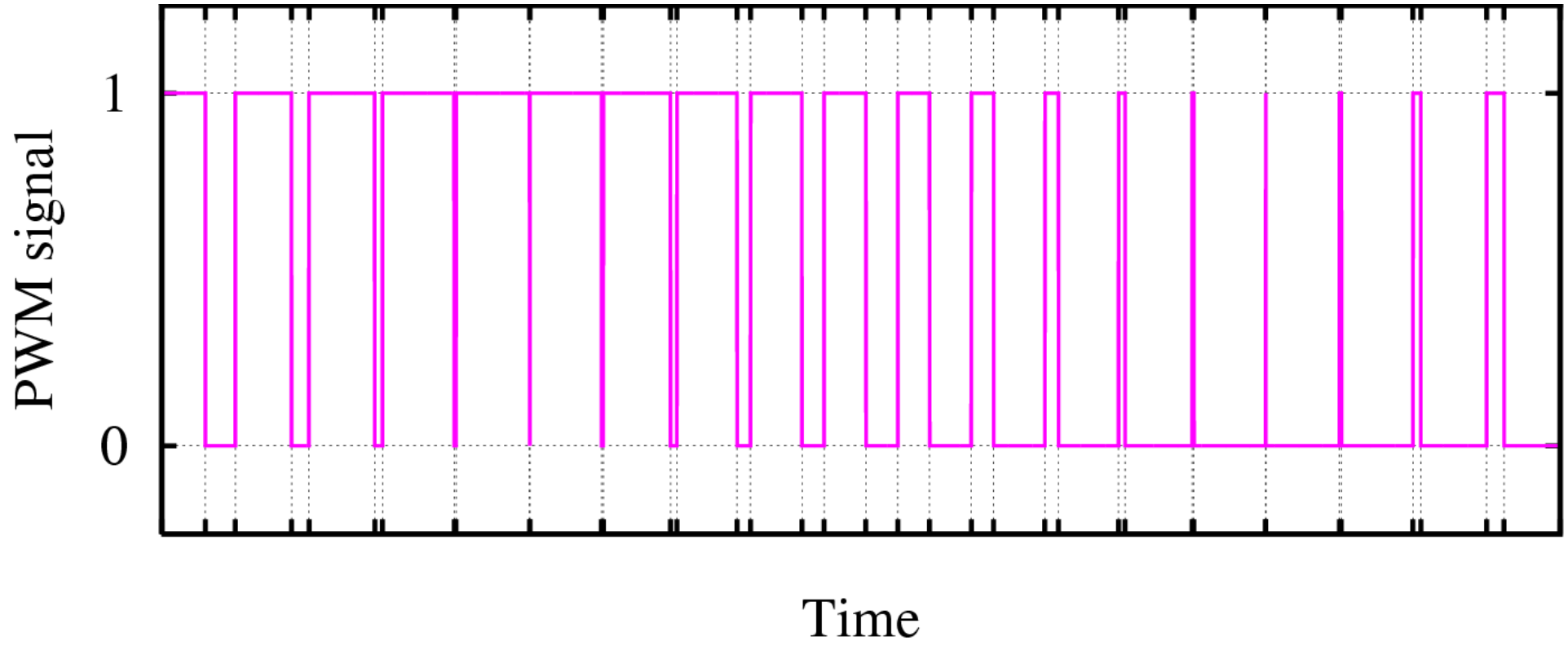
Electronic Speed Controllers (ESCs) are critical components in Unmanned Aerial Vehicles (UAVs) and other electrically powered remote-controlled or autonomous vehicles. In UAVs, ESCs are used for:

- Motor Control: They regulate the power delivered to the motors based on inputs from the flight controller or radio receiver.
- Efficiency and Precision: ESCs can provide precise control over motor speed, which is essential for the stability and maneuverability of the UAV. This precise control is achieved through rapid switching (PWM - Pulse Width Modulation) of the power supply to the motors.
- Braking: Some ESCs have braking features that can quickly stop the motor, which is useful in certain maneuvers or when the UAV needs to be quickly stabilized.

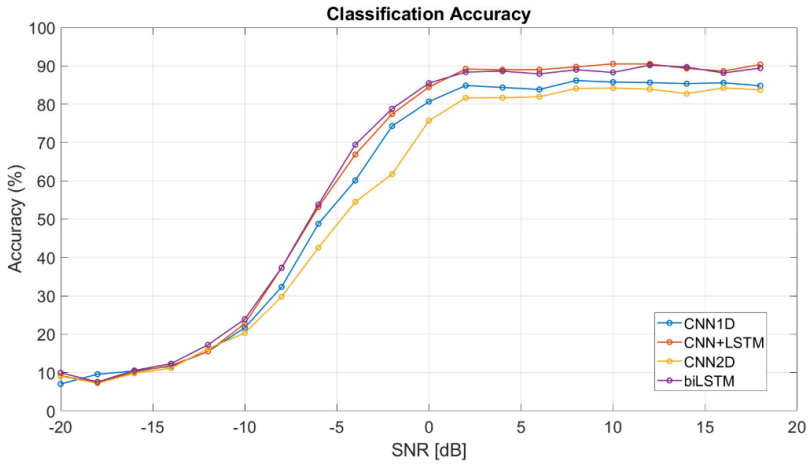


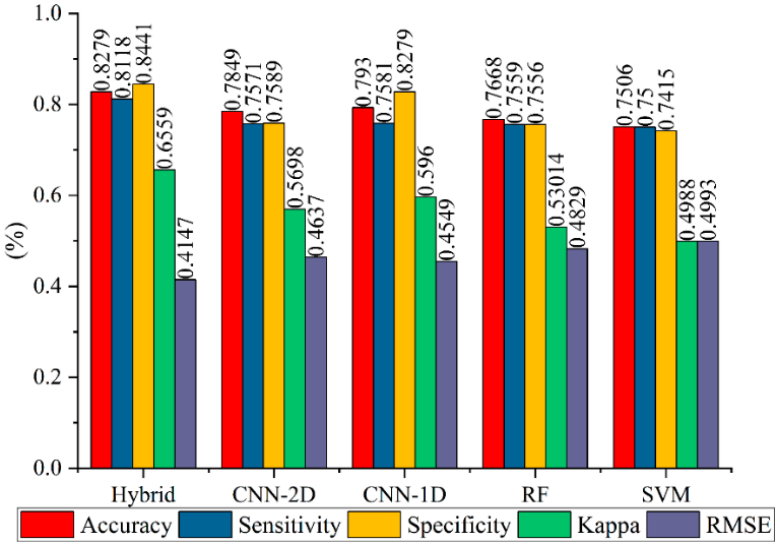
Pulse Width Modulation (PWM)

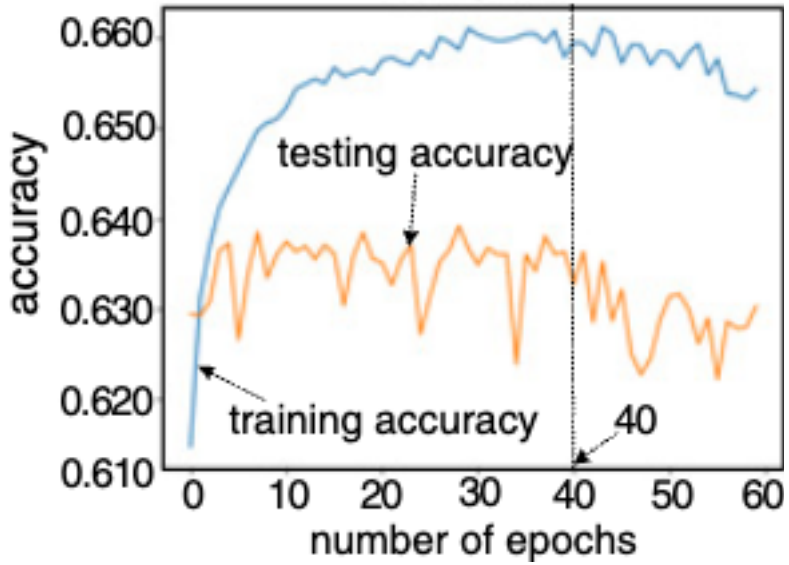
Pulse Width Modulation (PWM) signals are a method used to control the amount of power delivered to the rotors.



Related Work







Simon et al. [1] applied deep learning to combat UAV jamming and deception attacks using telecommunication features.

Yang et al. [2] proposed a hybrid model using CNN-2D, CNN-1D, RF, and SVM for landslide prediction. Despite achieving 82.79% accuracy, their model's dependence on high-quality, correlated input data may not be feasible in all UAV operational environments.

Lerman et al. [3] demonstrated the utility of machine learning to exploit UAV system vulnerabilities through side channel signals. They haven't used PWM signals.

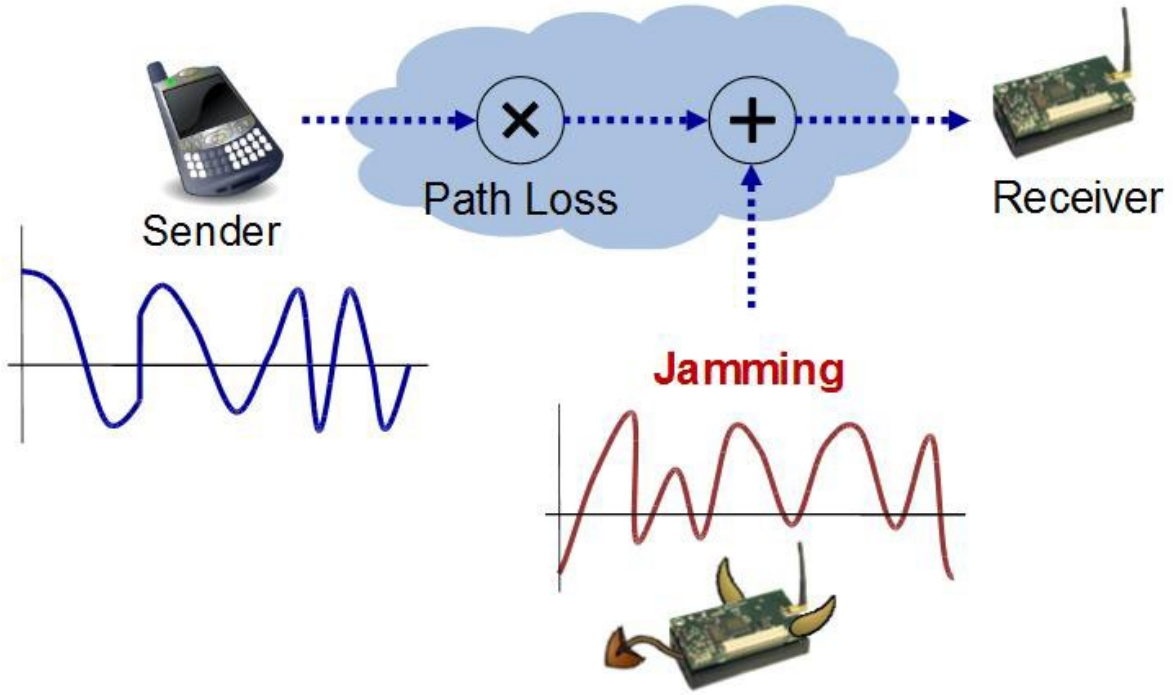
[1] Ond˘rej ˘Simon and Tom´a˘s G¨otthans. A Survey on the Use of Deep Learning Techniques for UAV Jamming and Deception. Electronics, 11(19):3025, September 2022.

[2] Xin Yang, Rui Liu, Mei Yang, Jingjue Chen, Tianqiang Liu, Yuantao Yang, Wei Chen, and Yuting Wang. Incorporating landslide spatial information and correlated features among conditioning factors for landslide susceptibility mapping. Remote Sensing, 13(11):2166, 2021.

[3] Liran Lerman, Romain Poussier, Olivier Markowitch, and Franc¸ois- Xavier Standaert. Template attacks versus machine learning revisited and the curse of dimensionality in side-channel analysis: extended version. Journal of Cryptographic Engineering, 8:301–313, 2018

Research Gap

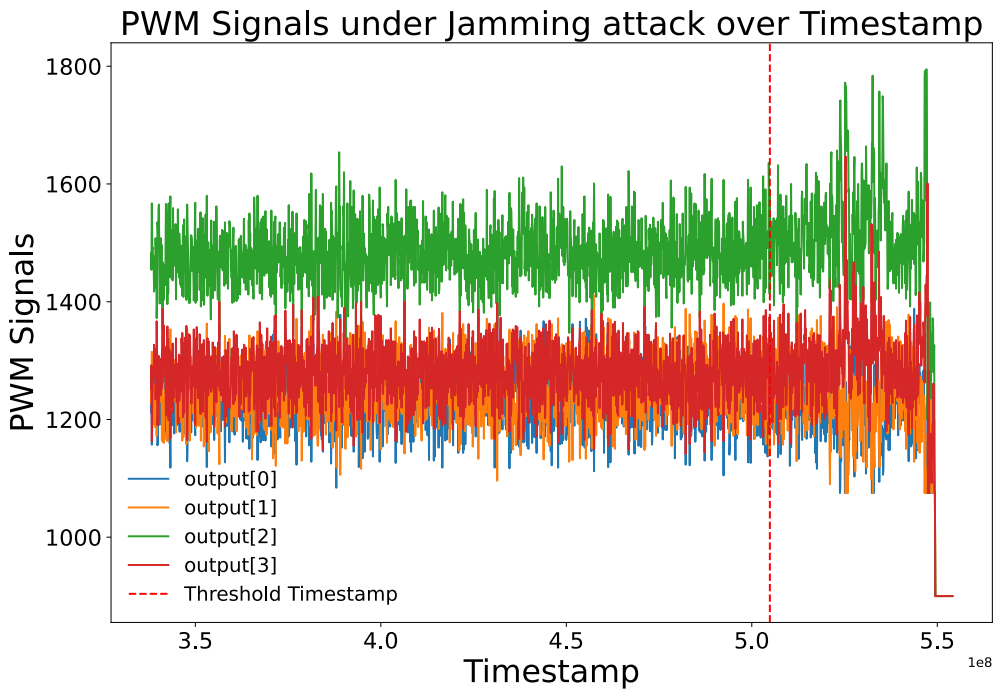
- Conventional Unmanned Aerial Vehicle (UAV) Intrusion Detection Systems (IDS) primarily focus on
  - Network traffic analysis
  - GPS signal integrity
  - Behavioral patterns
- One critical gap in current UAV IDS is the lack of utilization of Pulse Width Modulation (PWM) signals for attack detection.

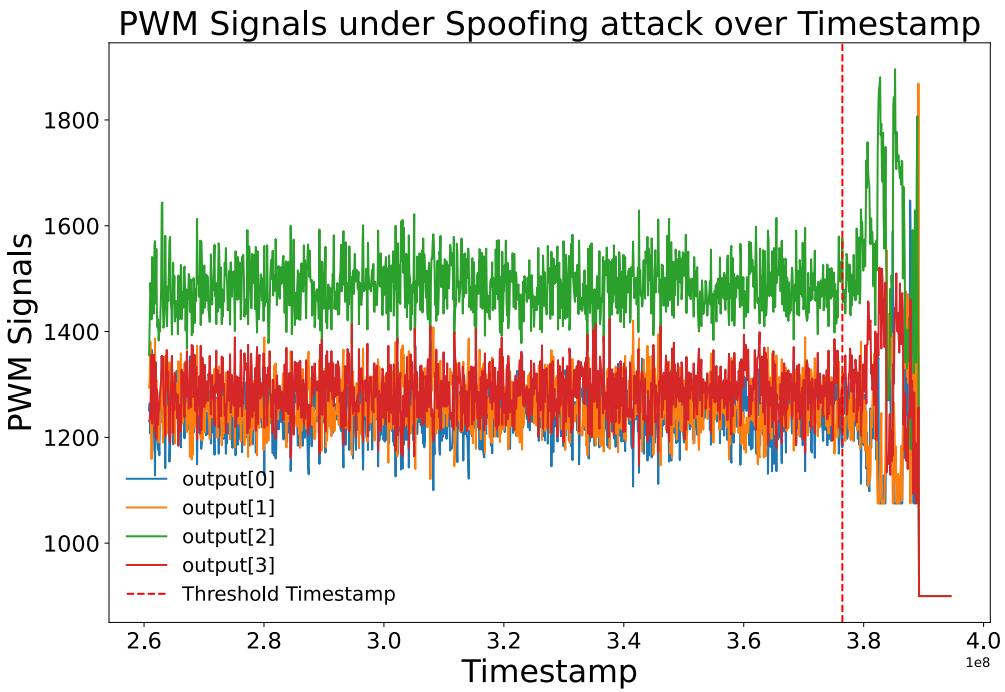


Threat Model

Jamming Attack
UAV GPS receives no signals of current location. It can lead to a crash.

Spoofing Attack
UAV GPS receives a corrupted location. It can lead to a crash or redirect the UAV.



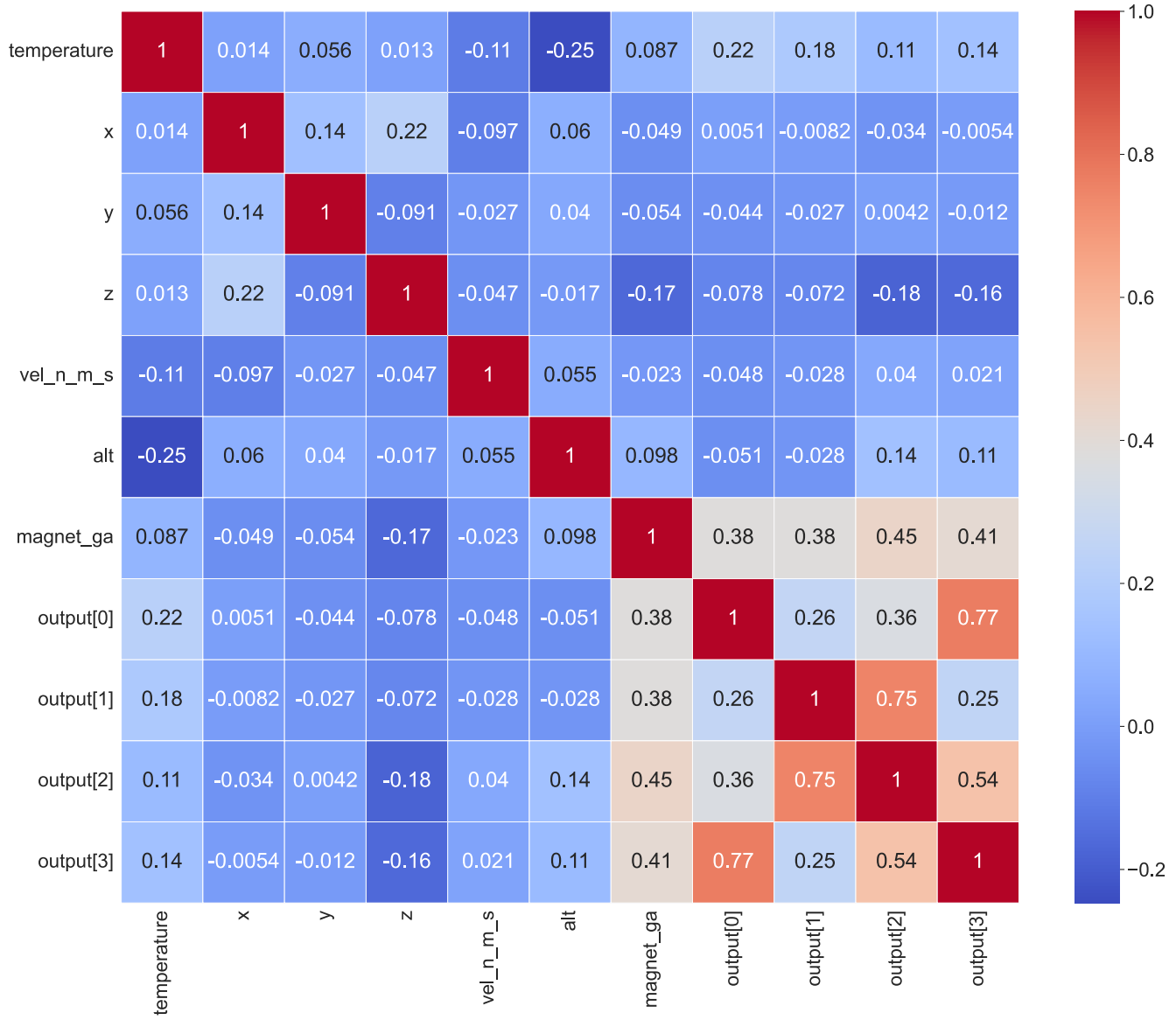


PWM under Jamming & Spoofing attack

Are PWM correlated to Sensor-based IDS features?

PWM signals have almost a value of 0 in correlation with sensors features.

Only values above 0.5 or lower than -0.5 can be considered correlated.



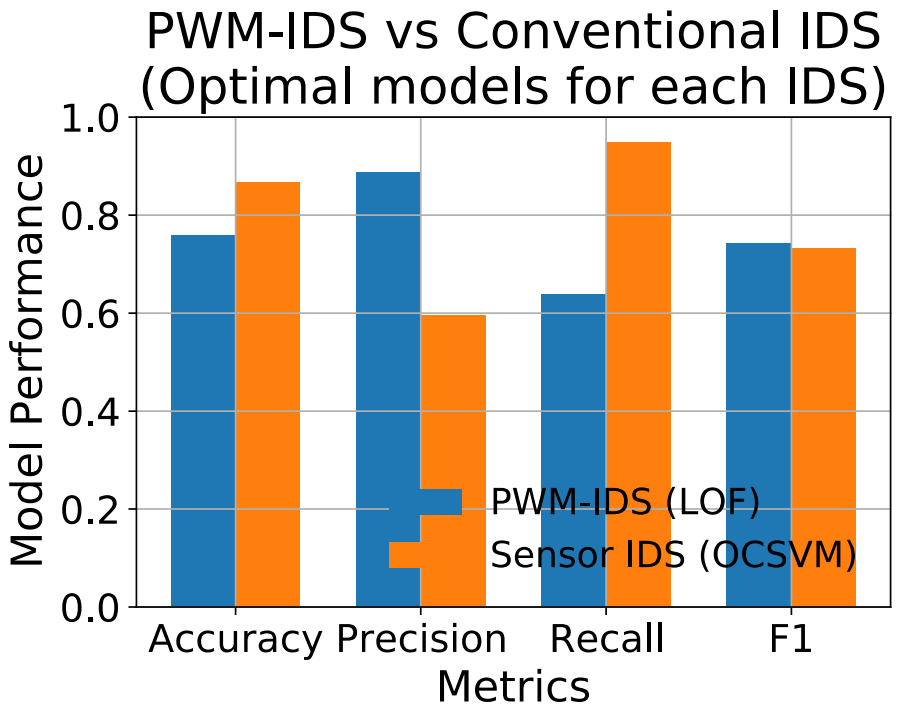
Dataset

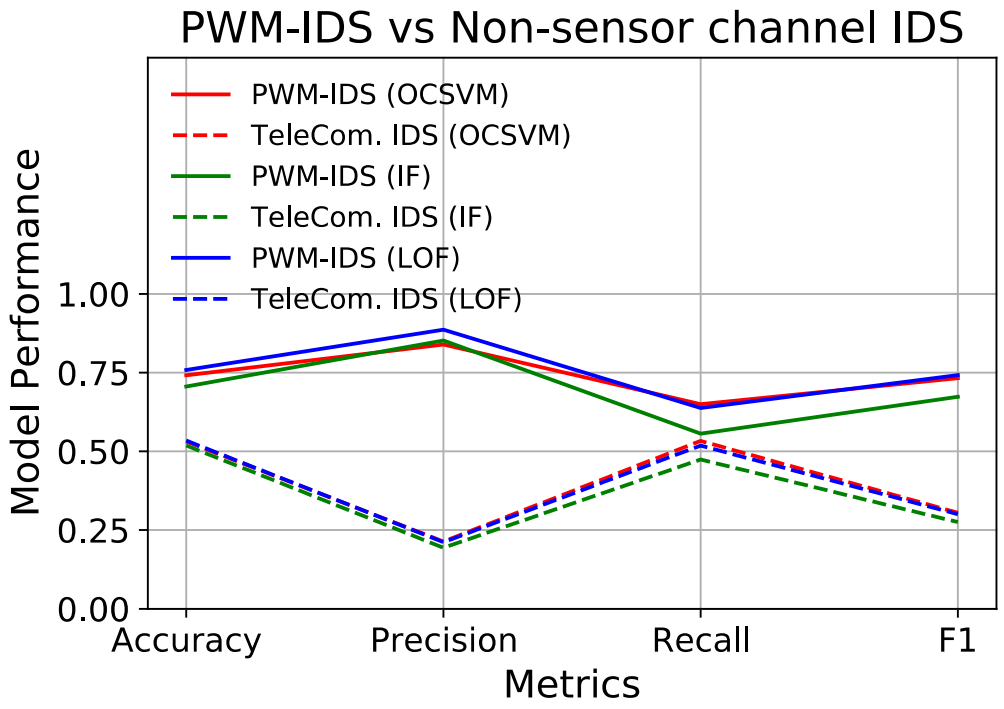
	Jamming	Spoofing	Total
Benign	1668	1156	2824
Malicious	493	181	674
Total	2161	1337	3498

Hardware-in-the-loop simulation has been done to generate over 3000 samples of UAV operations in normal operations and under attack.

PWM IDS Comparison to Other IDSs

The main metrics scores are similar between conventional Sensors IDS with our proposed IDS. In addition, our IDS over performs a Telecommunication based IDS.





Performance Comparison

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%

Can the Physical layer data be used to detect attacks in real-time?

- Our proposed IDS contrasts other channel IDSs by emphasizing the physical layer attributes, such as:
  - Signal strength
  - Frequency hopping patterns
  - 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.

Future Directions

- Live IDS to prove on-board the performance metrics obtained on ground.
- Add more attack vectors to the IDS.


Q&A