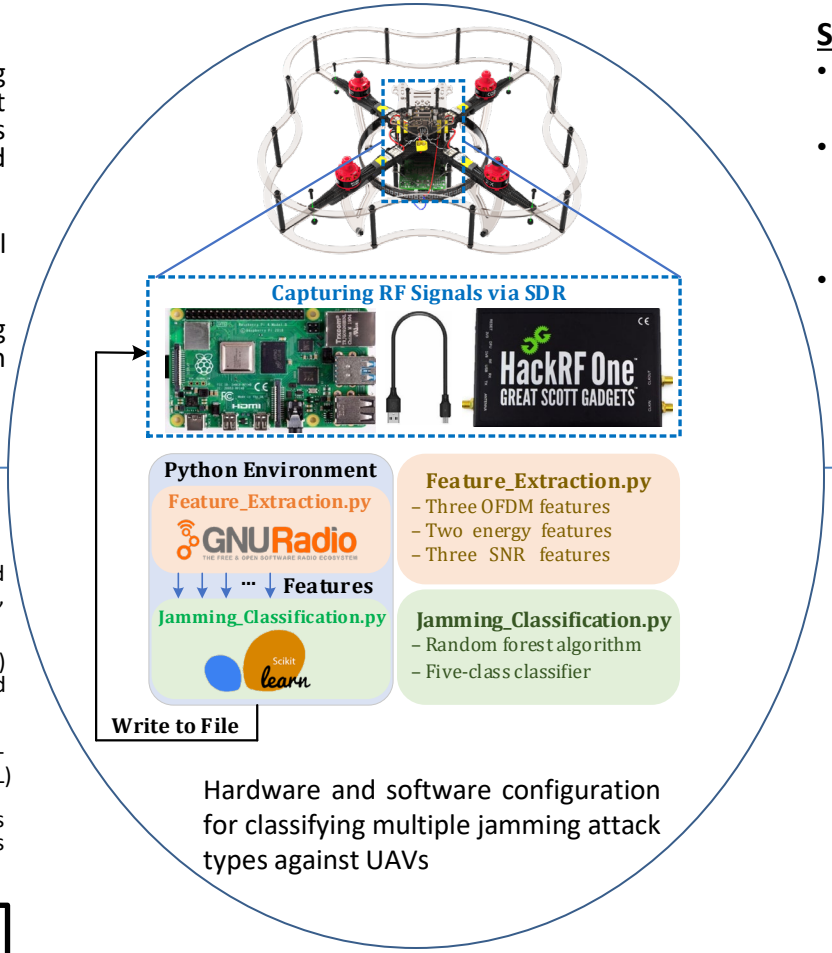
Jamming Detection and Classification in OFDM-based UAVs via Feature- and Spectrogram-tailored Machine Learning

PURDUE UNIVERSITY NORTHWEST

Challenge

- To Develop real-time jamming detection/mitigation methods that comply with existing UAV standards and facilitate high detection and low false-alarm rates
- These methods must impose minimal software/hardware modifications
- These methods must allow jamming classification to identify the optimum countermeasure protocol



Hardware and software configuration for classifying multiple jamming attack types against UAVs

Solution

- Multiple jamming types are explored qualitatively for their launch complexity, jamming range, and severity
- Signal features (e.g., SNR, OFDM parameters) are used for developing feature-based classification via machine learning (ML)
- Spectrograms are used to build image-based classification via deep learning (DL)
- The performance of both approaches is analyzed quantitatively with metrics including detection and false alarm rates

NSF award no. 2006662 | Dr. Khair Al Shamaileh (PI) | Purdue University Northwest

E-mail: kalshama@pnw.edu

https://github.com/michaelevol/uavs_jamming_detection

Scientific Impact

- Three publications in technical journals and conference proceedings
- Datasets of features and spectrograms for four jamming types made public. Datasets convey actual measurements during realistic attack setups
- ML/DL models and attack generation files made public. These may be used to boost cybersecurity and ML research in other domains (e.g., smart grids, Internet of Things)

Broader Impact

- At least 15 undergraduate and graduate students, including those from minority groups, have worked on this project and other projects funded by NSF award no. 2006662
- Research outcomes disseminated in summer camps with +50 students from at least four states
- Research outcomes integrated with the PI dual-level course (i.e., Wireless Communications, Spring 2022 offering, 12 students)
- With the increase in the use of UAVs, sensitive data and quality of service can be compromised by attackers. Hence, cyber-secure UAV networks with robust defense mechanisms (i.e., detection, mitigation) promote public safety