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

Khair Al Shamaileh, Purdue University Northwest

https://github.com/michaelevol/uavs_jamming_detection

Background: Recently, unmanned aerial vehicles (UAVs) have been widely adopted in various applications such as climate monitoring, disaster management, merchandise delivery, search and rescue operations, space exploration, and wildlife tracking. However, in these applications, little attention has been paid to the cybersecurity aspect. For example, cyberattacks (e.g., jamming, location spoofing) compromise the performance of UAVs, or even lead to catastrophic consequences. Thus, developing UAV-tailored cyberattack detection/mitigation methods are particularly significant

Challenge

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

Solution: Multiple jamming types are explored qualitatively for their launch complexity, range, and severity. Signal features (e.g., SNR, OFDM parameters) are used to develop feature-based classification via machine learning (ML). Also, 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

Scientific Impacts

- Journals and conference Publications
  - "Real-time classification of jamming attacks against UAVs via on-board software-defined radio and machine learning-based receiver module, *IEEE Electro-information Technology, Conference*, 2022 (accepted)
  - "Jamming detection and classification in OFDM-based UAVs via feature- and spectrogram-tailored machine learning," *IEEE Access,* vol. 10, pp. 16859-16870, 2022
  - "A machine learning approach for detecting and classifying jamming attacks against OFDM-based UAVs," *ACM Workshop on Wireless Security and Machine Learning*, 2021
- Datasets of features and spectrograms for four jamming types made public. Datasets convey actual measurements during realistic attack setups
- ML/DL models and attack files made public. These may be used to boost cybersecurity/ML research in other domains (e.g., smart grids, IoT)

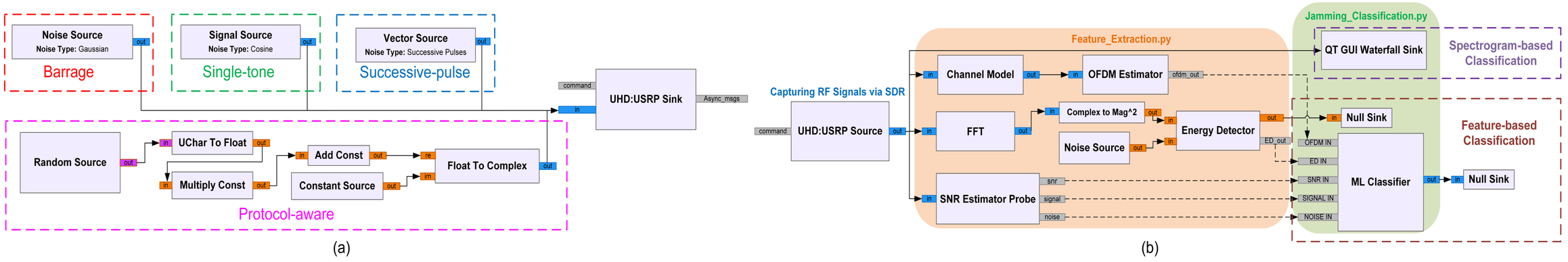

Figure 1: Simplified GNURadio flowgraphs for (a) launching jamming attacks and (b) receiver module for extracting signal features or spectrogram images and executing jamming detection/classification

Table 1: Metrics of the feature-based jamming detection models (VA: validation accuracy, DR: detection rate, FS: F-score, CTR: CPU training time, CTE: CPU testing time)

Performance metrics for five-class models											
	Case 1: Nine Features			Case 2: Eight Features			Case 3: Seven Features			Time (Case 2)	
ML Classifier	VA (%)	DR (%)	FS	VA (%)	DR (%)	FS	VA (%)	DR (%)	FS	CTR(sec)	CTE(sec)
LR	82.45 (± 0.65)	82.90	0.82	82.75 (± 0.67)	82.73	0.82	79.42 (± 0.76)	78.95	0.79	0.860	0.002
KNN	84.47 (± 0.74)	84.23	0.84	84.87 (± 0.74)	83.50	0.84	83.70 (± 0.72)	83.40	0.83	0.131	0.130
NB	79.30 (± 0.80)	78.74	0.79	79.40 (± 0.80)	78.33	0.78	77.50 (± 0.79)	77.80	0.77	0.002	3.550
DT	91.60 (± 0.70)	92.52	0.93	91.90 (± 0.64)	91.75	0.92	84.96 (± 0.75)	84.75	0.85	0.058	≈ 0
RF	**91.80 (± 0.06)**	**92.11**	**0.92**	**92.20 (± 0.60)**	**92.20**	**0.92**	**86.23 (± 0.79)**	**85.95**	**0.86**	**5.404**	**0.411**
MLP	78.02 (± 1.70)	79.60	0.79	77.50 (± 2.13)	76.25	0.75	77.46 (± 1.80)	75.60	0.72	1.807	0.005
Performance metrics for two-class models											
LR	**100.00 (± 0.00)**	**100.00**	**1.00**	**100.00 (± 0.00)**	**100.00**	**1.00**	**100.00 (± 0.00)**	**100.00**	**1.00**	**0.022**	**0.003**
KNN	99.92 (± 0.07)	99.89	1.00	99.93 (± 0.06)	99.94	1.00	99.93 (± 0.06)	99.96	1.00	0.135	0.135
NB	99.80 (± 0.09)	99.79	1.00	99.77 (± 0.12)	99.85	1.00	99.77 (± 0.11)	99.86	1.00	0.006	≈ 0
DT	100.00 (± 0.02)	99.98	1.00	100.00 (± 0.02)	99.98	1.00	99.98 (± 0.03)	100.00	1.00	0.009	≈ 0
RF	**100.00 (± 0.00)**	**100.00**	**1.00**	**100.00 (± 0.00)**	**100.00**	**1.00**	**100.00 (± 0.00)**	**100.00**	**1.00**	**2.344**	**0.203**
MLP	99.72 (± 0.60)	99.98	1.00	99.23 (± 2.50)	99.98	1.00	99.70 (± 0.50)	99.89	1.00	1.112	0.001

Table 2: Metrics of the spectrogram-based DL models (VA: validation accuracy, DR: detection rate, FS: F-score, GTR: GPU training time, GTE: GPU testing time, CTR: CPU training time, CTE: CPU testing time)

Performance metrics for five-class models							
ML Classifier	VA (%)	DR (%)	FS	GTR (sec)	GTE (sec)	CTR (sec)	CTE (sec)
AlexNet	100.00	99.36	0.99	174	0.82	6765	4.90
VGG-16	94.03	94.50	0.94	1479	5.81	70932	63.30
ResNet-50	99.82	98.10	0.98	1118	2.72	58359	31.84
EfficientNet-B0	**98.55**	**99.79**	**1.00**	**1530**	**2.53**	**39476**	**31.22**
Performance metrics for two-class models							
ML Classifier	VA (%)	DR (%)	FS	GTR (sec)	GTE (sec)	CTR (sec)	CTE (sec)
AlexNet	100.00	99.15	0.99	171	0.76	6048	4.86
VGG-16	99.91	99.36	0.99	1478	5.77	52837	63.43
ResNet-50	100.00	99.36	0.99	1114	2.47	52334	32.00
EfficientNet-B0	**99.91**	**100.00**	**1.00**	**1489**	**2.28**	**39351**	**31.55**

Impact on Society: 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

Impact on Educational Outreach

- At least 15 undergraduate/graduate students, including minority, have worked on this project and other projects funded by NSF award 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)