GPS Spoofing/Mimicking Attacks on UAS: Detection Techniques Based on Machine and Deep Learning

Naima Kaabouch, University of North Dakota

https://github.com/ghilasaissou/GPS_Spoofing_on_UAS

Unmanned Aerial Systems (UAS) rely primarily on the Global Positioning System (GPS) for navigation. Unencrypted civilian GPS signals, however, are vulnerable to a variety of threats, including jamming, injection, and GPS spoofing/mimicking attacks. This project aims at developing artificial intelligence models for detecting and mitigating several attacks targeting UAS, including GPS spoofing attacks.

Challenge

- Sophisticated GPS spoofing/mimicking attacks are difficult to detect.
- Development of robust and real-time techniques to detect GPS spoofing attacks.
- Development of fast and light weight models to accommodate the Weight, Power, and Size (SWaP) constraints of UAS.
- Models must also introduce minor hardware and software adjustments to GPS receivers.

Solution

- Collection of real GPS signals and different forms of GPS spoofing attacks with varying stealth and complexity are simulated.
- Multiple features are extracted to build a dataset and train models.
- Performance comparison of supervised and unsupervised machine learning models is investigated using several metrics consistent with the characteristics and constraints of UAS.

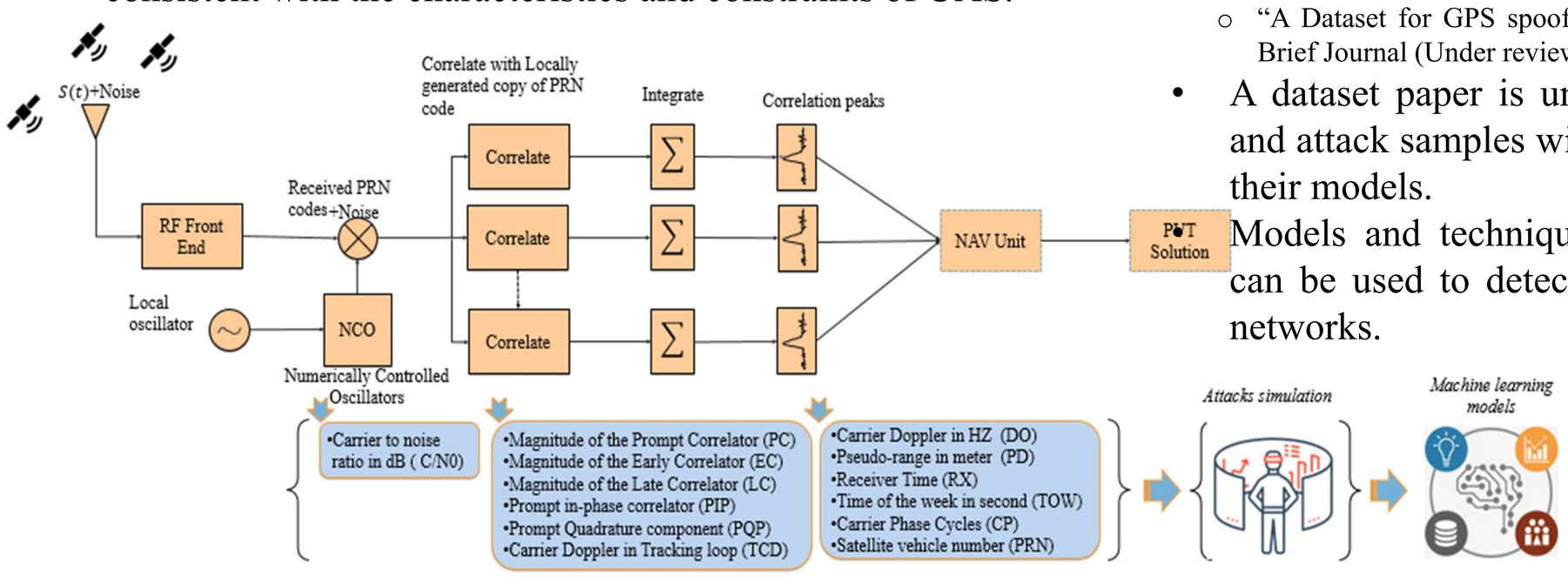

Figure 1: GPS spoofing attack detection model.

		DT	RF	Logistic regression	C-SVM	KNN	GaussianNB
Accuracy(%)		94.01	**94.52**	75.68	84.67	80.32	44.35
PFA(%)		12.89	**13.23**	42.46	27.13	34.92	43.51
Precision (%)	Authentic signals	87.84	**99.70**	81.94	93.17	88.27	34.06
	Simplistic attack	90.79	**89.98**	76.54	75.77	72.73	52.45
	Intermediate attack	99.97	**89.78**	67.88	81.58	76.85	60.30
	Sophisticated attack	98.90	**99.98**	78.14	91.58	86.64	47.11
POD (%)	Simplistic attack	99.20	**98.11**	83.86	89.98	87.89	19.22
	Intermediate attack	90.13	**93.25**	70.90	81.38	77.15	38.87
	Sophisticated attack	99.61	**99.96**	86.63	94.48	90.90	63.19
PMD (%)	Simplistic attack	0.80	**1.90**	16.14	21.28	12.11	80.78
	Intermediate attack	9.86	**6.75**	29.1	18.62	22.85	61.13
	Sophisticated attack	0.29	**0.04**	10.37	5.53	9.10	36.81

		DT	KNN	RF	C-SVM	LR	GaussianNB
Processing time (s)	Training	1.42	0.42	191.40	354.68	458.59	**0.05**
	Detection	**0.01**	13.30	5.72	131.61	0.04	0.02
Memory size (MiB)	Training	**1.55**	9.44	286.98	8.65	91.51	1.58
	Detection	0.38	1.15	**0.02**	0.94	0.60	3.77

Figure 2: Example of results.

Scientific Impacts

- Seven (7) papers have been published/submitted in and to technical journals and conference proceedings.
  - "Dynamic Selection Techniques for Detecting GPS Spoofing Attacks on UAVs." *Sensors* 22, no. 2 (2022): 662.
  - "Instance-based Supervised Machine Learning Models for Detecting GPS Spoofing Attacks on UAS." Computing and Communication Workshop and Conference (CCWC), pp. 0208-0214. IEEE, 2022.
  - "A Comparative Analysis of the Ensemble Models for Detecting GPS Spoofing attacks on UAVs." IEEE Computing and Communication Workshop and Conference (CCWC), pp. 0310-0315. IEEE, 2022.
  - "Tree-Based Supervised Machine Learning Models for Detecting GPS Spoofing Attacks on UAS." IEEE Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), pp. 0649-0653. IEEE, 2021.
  - "A Comparative Analysis of the Ensemble Models for Detecting GPS Spoofing attacks on UAVs." *Computing and Communication Workshop and Conference (CCWC)*, pp. 0310-0315. IEEE, 2022.
  - "Simulation Testbeds and Frameworks for UAV Performance Evaluation." IEEE International Conference on Electro Information Technology (EIT), pp. 335-341. IEEE, 2021.
  - "A Dataset for GPS spoofing detection on UAS," Elsevier Data in Brief Journal (Under review).
- A dataset paper is under review to share real GPS and attack samples with researchers to study and test their models.
- Models and techniques resulting from this project can be used to detect attacks in other systems and networks.

Impact on Educational Outreach

- Project provided research opportunities to seventeen (17) graduate and undergraduate students.
- Project outcomes shared with hundreds of K-12 and engineering students who attended the 2022 Collegiate Drone Racing Championship and the 2021 UAS Summit & Expo.

Impact on Society

UAS applications are rising in civilian and military domains. However, they are prone to several cyber-attacks that can lead to collisions and casualties. Therefore, robust detection and mitigation techniques are highly needed to preserve the safety of civilians and infrastructure.