UNIVERSITY OF NORTH DAKOTA

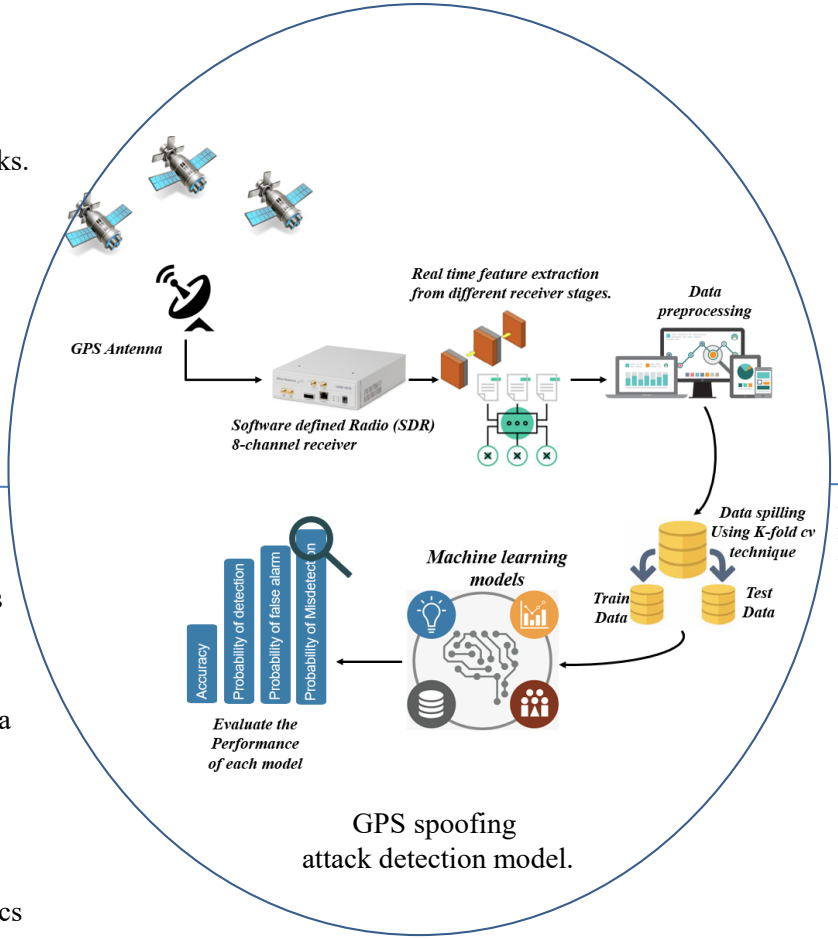
GPS Spoofing Attacks on UAS: Detection Techniques Based on Machine and Deep Learning

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.



GPS spoofing attack detection model.

Scientific Impact

- Seven (7) papers have been published in technical journals and conference proceedings.
- Three (3) journal papers have been submitted.
- A GPS dataset paper is under review to share real GPS and attack samples with researchers to study and test their models.

Broader Impact and Broader Participation

- Models and techniques resulting from this project can be used to detect GPS spoofing attacks in other systems that carry GPS devices.
- The project provided research opportunities to seventeen (17) graduate and undergraduate students.
- Outreach Activities performed during two events: 2022 Collegiate Drone Racing Championship and the 2021 UAS Summit & Expo.

NSF award no. 2006674 | Dr. Naima Kaabouch (PI) | University of North Dakota
E-mail: naima.kaabouch@und.edu