IAF SPACE COMMUNICATIONS AND NAVIGATION SYMPOSIUM (B2)
Interactive Presentations - IAF SPACE COMMUNICATIONS AND NAVIGATION SYMPOSIUM (IP)

Author: Ms. Asra Mahroof
Institute of Space Technology (IST), Pakistan

Dr. Salma Zainab Farooq
Institute of Space Technology (IST), Pakistan
Mr. Imtiaz Nabi
Institute of Space Technology (IST), Pakistan

ENHANCED GNSS SPOOFING DETECTION USING MACHINE LEARNING: COMPARATIVE ANALYSIS OF KNN AND LOGISTIC REGRESSION MODELS

Abstract

The susceptibility of GNSS open service signals to spoofing presents a significant risk to users relying on safety-of-life applications. The Spoofer generates and transmits GNSS-like signals, leading to inaccurate position, velocity, and timing solution for an unaware user. In this paper, a GNSS spoofing detection methodology using machine learning (ML) techniques is proposed. The dataset, TEXBAT GPS L1 C/A spoofing scenario, is used to train ML models and the trained models are tested on spoofed and clean signals available. The features used for training are, DLL outputs and carrier to noise density ratio, obtained after tracking. The ML models utilized in this research are k-Nearest Neighbor (kNN) and Logistic Regression which perform binary classification for spoofing detection. The results are compared with the complex Support Vector Machine (SVM) model, and it is seen that the proposed method achieves comparable and even better performance. Our analysis aims to assess the accuracy of ML models in predicting spoofing attacks and determining the superior model.