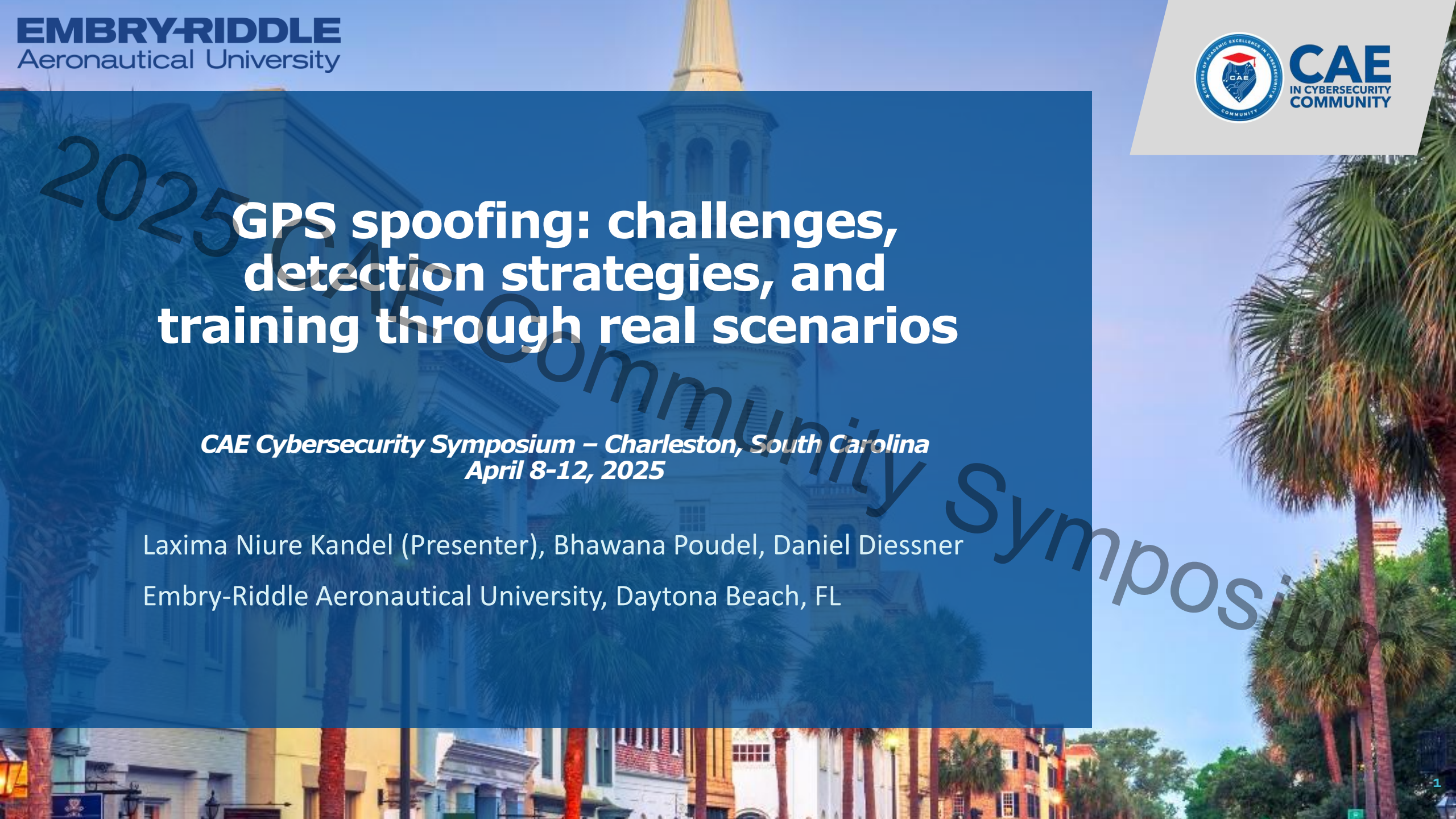


EMBRY-RIDDLE Aeronautical University

CAE IN CYBERSECURITY COMMUNITY

GPS spoofing: challenges, detection strategies, and training through real scenarios

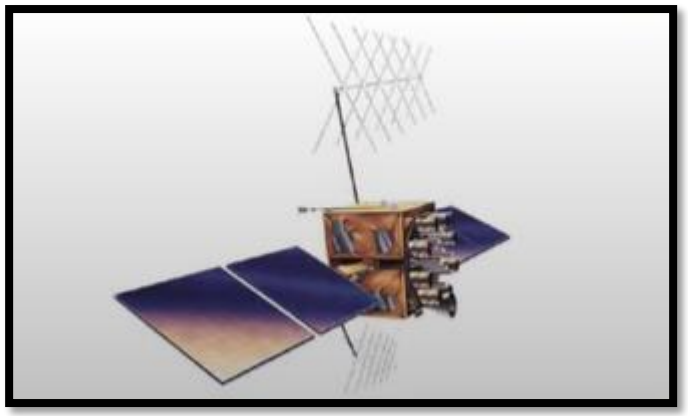
CAE Cybersecurity Symposium – Charleston, South Carolina
April 8-12, 2025

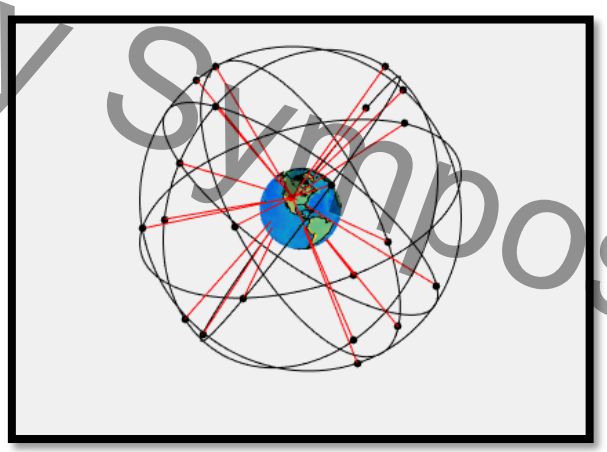
Laxima Niure Kandel (Presenter), Bhawana Poudel, Daniel Diessner

Embry-Riddle Aeronautical University, Daytona Beach, FL

What is Global Positioning System (GPS) ?

- Constellation of space vehicles (SVs) and ground control stations managed by the US Space Force
  - Provides **position, navigation, and timing (PNT)** data to military and civilian users globally 24/7/365
- GPS satellites (currently 31 satellite in orbit): transmit time, satellite location to the user
- User needs at least four satellites in view to determine time error; three after correcting





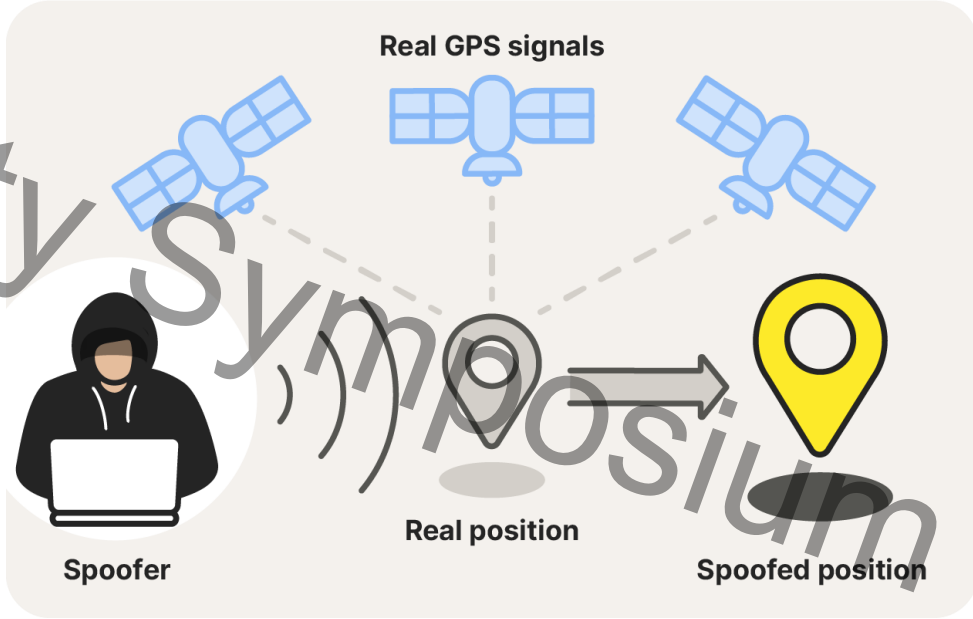
https://commons.wikimedia.org/w/index.php?curid=47209685

What is GPS Spoofing?

Spoofing: Generation of fake signals that mimic those from GPS satellites causing GPS receivers to calculate incorrect PNT information

Techniques:

- Source signal spoofing
  - Alter the characteristics (amplitude, frequency, phase shift, etc.) of the incoming signal from satellite
- Receiver spoofing
  - Attack the receiver's ability to decode the signal



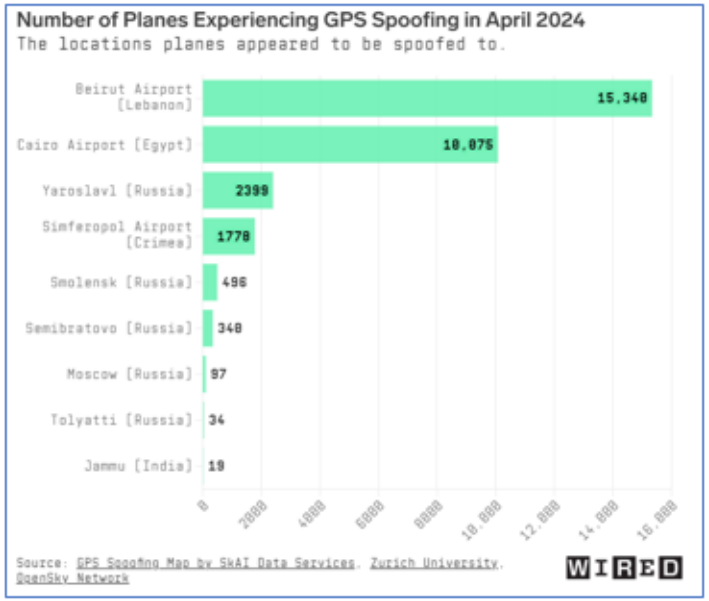
Real-World GPS Spoofing Incidents

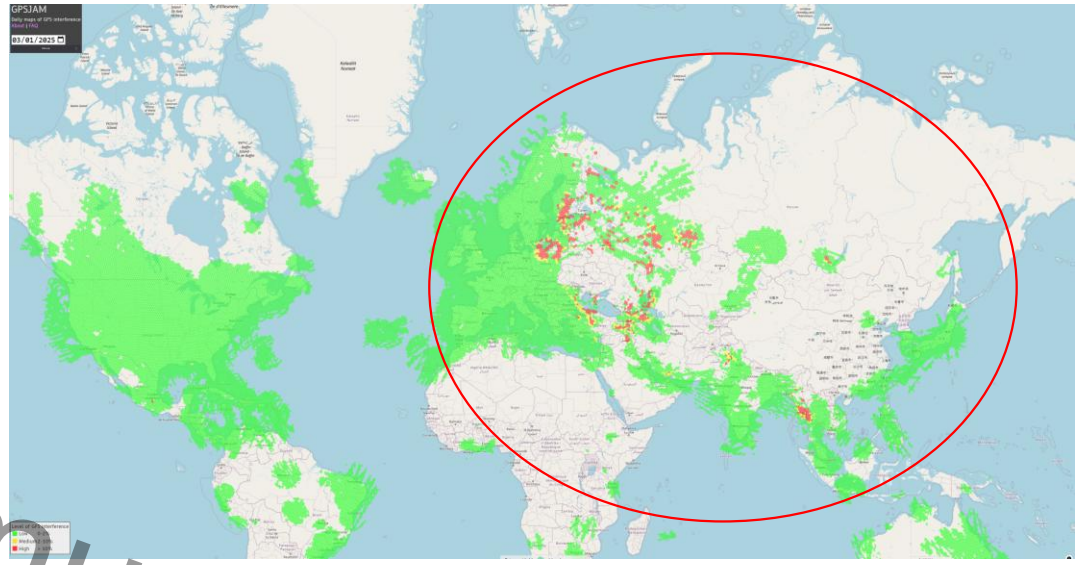
FORBES > BUSINESS > AEROSPACE & DEFENSE

GPS Spoofing in the Middle East Is Now Capturing Avionics

Avionics like those equipping Bombardier's Global 7500 business jet and other commercial aircraft are being "captured" by false GPS broadcasts in the Middle East. [-] BOMBARDIER

"What we've seen since late September," University of Texas researchers say," is unprecedented. We have never seen commercial aircraft captured by GPS spoofing before."





Credit: INCD / El Al

Detection of GPS Spoofing ?

Spoofing Detection

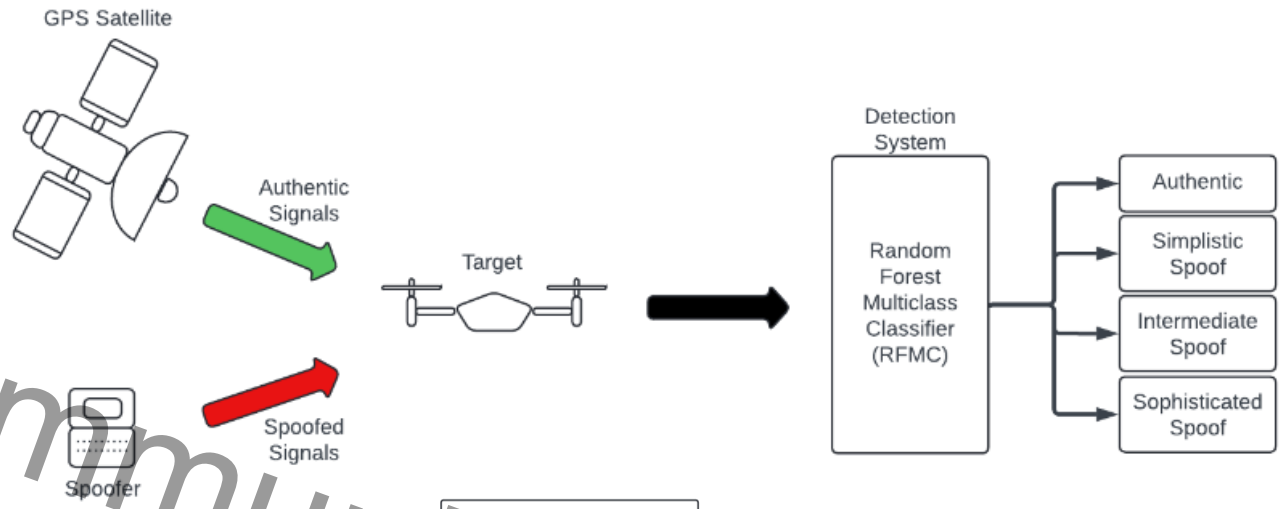
- Dual/multi-band receivers (to compare signals from different bands)
- Global Navigation Satellite System (GNSS) receivers (compare signals from different constellations)
- Signal to Noise Ratio Analysis
- Power Level Checks

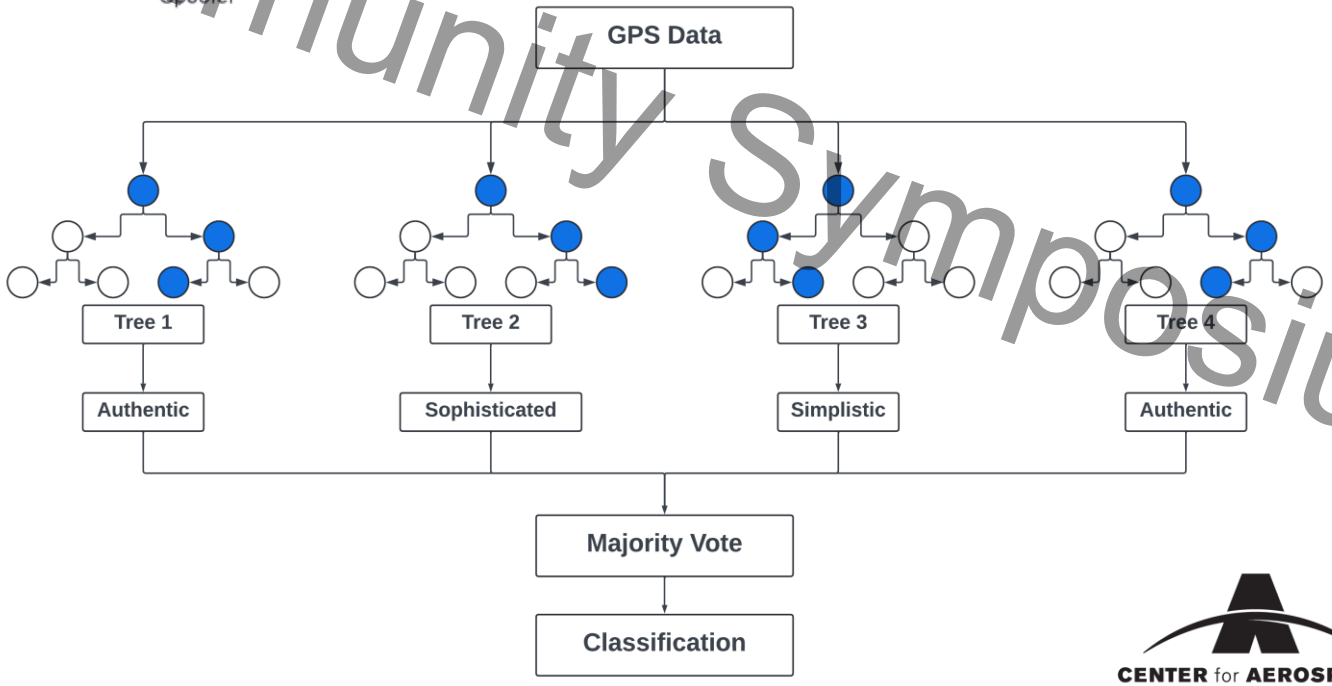
Machine Learning?

Machine Learning-Based GPS Spoofing Detection

Random Forest Multiclass Classification

- Apply the Random Forest Multiclass Classification Approach for the detection of the GPS spoofing signals
- Categorizing the GPS signals as:
  - Authentic Signal
  - Spoofed Signal
  - Simplistic
  - Intermediate
  - Sophisticated





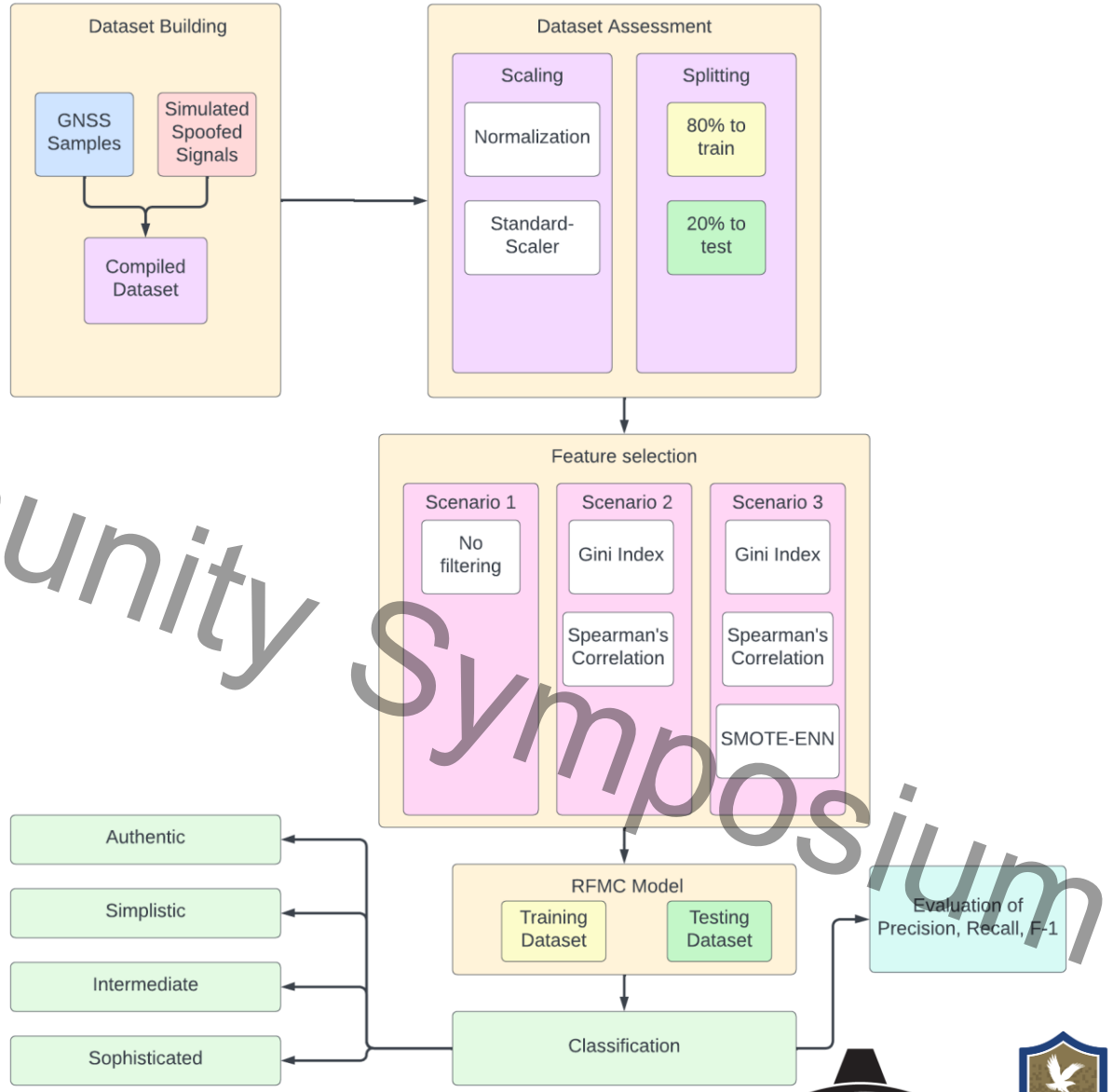
Methodology Overview

1. GPS Data
2. Data Scaling and Splitting
3. Feature Selection
4. Random Forest Classifier Model
5. Performance Evaluation

GPS Data

Collected by the School of Electrical Engineering and Computer Science, University of North Dakota; 510,530 samples, 13 features

Sample Type	Number of Samples	Percentage
Authentic signal	397825	78%
Simple spoofing	36458	7%
Intermediate spoofing	44232	9%
Sophisticated spoofing	32015	6%



Features in GPS Dataset

Extracted features	Abbreviations
Carrier to Noise Ratio	C/N_0
Early Correlator	EC
Late Correlator	LC
Prompt Correlator	PC
Prompt in-phase correlator	PIP
Prompt Quadrature component	PQP
Carrier Doppler in Tracking loop	TCD
Carrier Doppler	DO
Pseudo-range	PD
Receiver Time	RX
Time of the week	TOW
Carrier Phase Cycles	CP
Satellite vehicle number	PRN

13 total features are present in the dataset

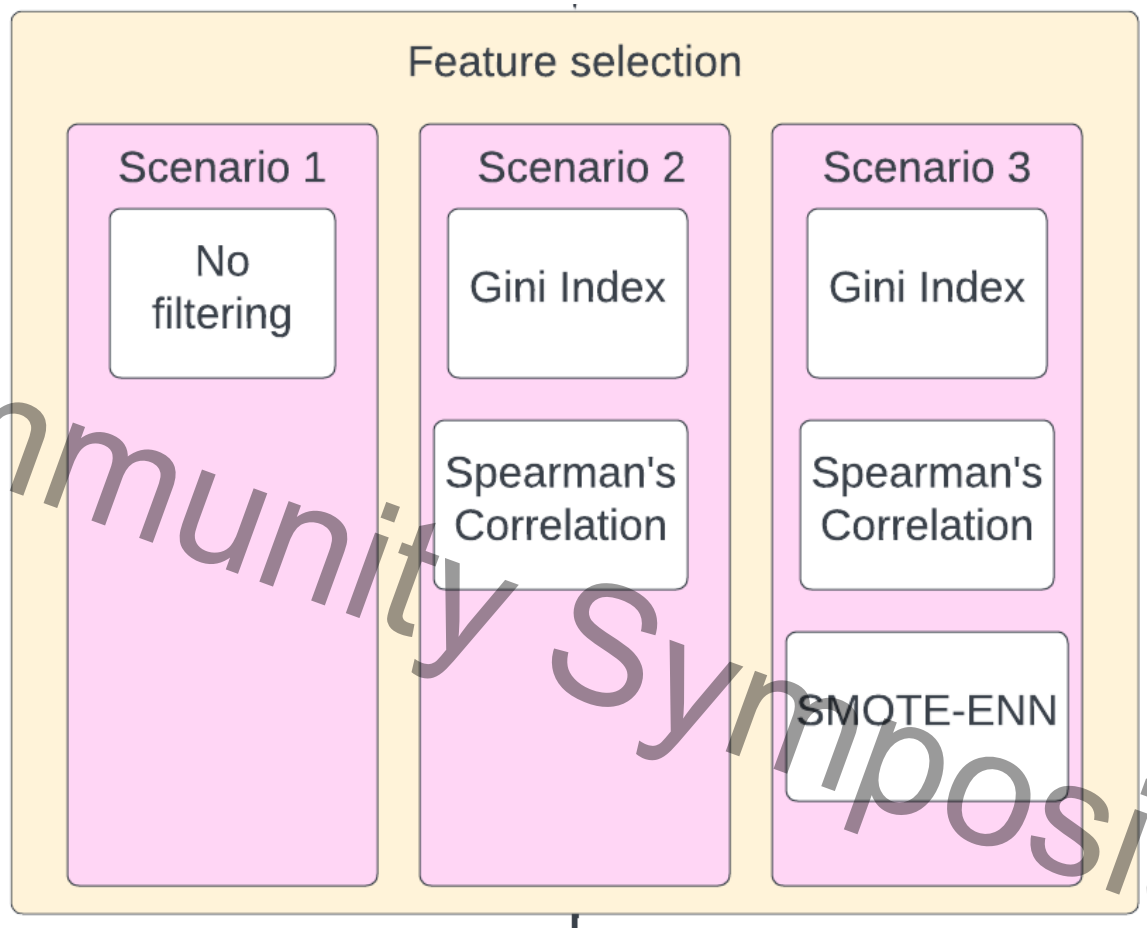
Features Selection

Scenario 1: All 13 features using Standard- Scaler

Scenario 2 Utilized 9 features, identified using the Gini index and utilized Spearman's correlation.

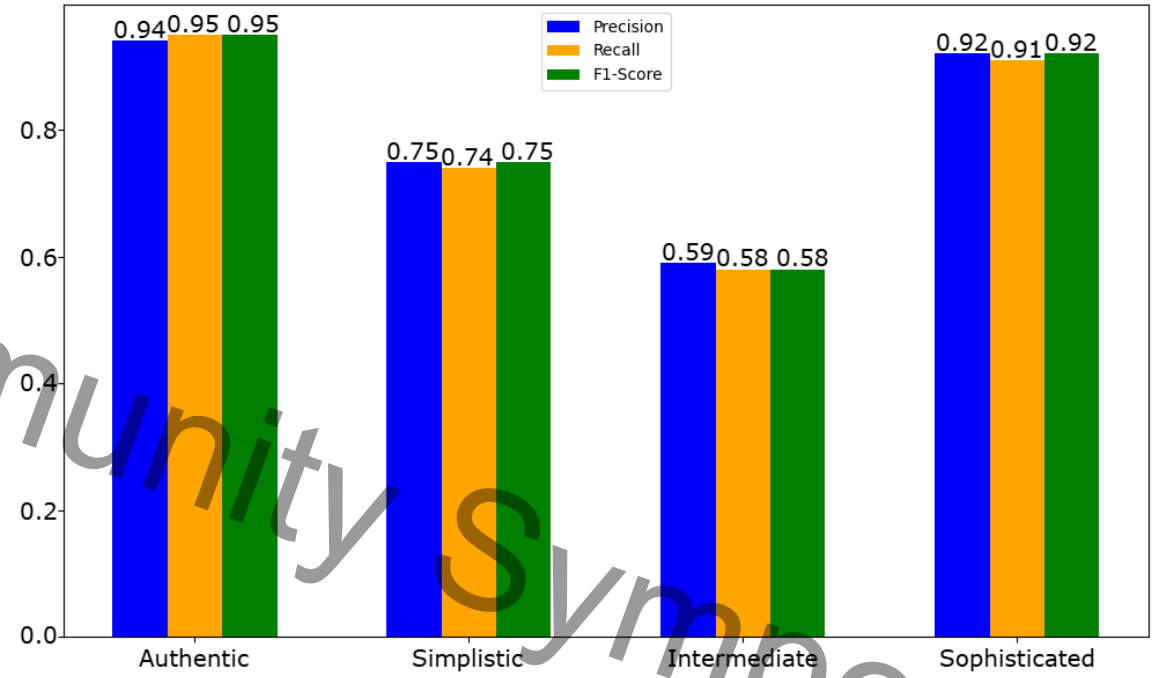
Scenario 3 Utilized 9 features collected from scenario two and used the SMOTE-ENN sampling technique to balance the dataset

SMOTE-ENN oversamples minority classes and under samples the majority class to address class imbalance



Results: Scenario 1

- Was accurately able to distinguish authentic and sophisticated signals (>0.90)
- Was moderate at classifying simplistic spoofing signals (~0.75)
- Demonstrated poor accuracy in classifying intermediate spoofing signals (~0.58)



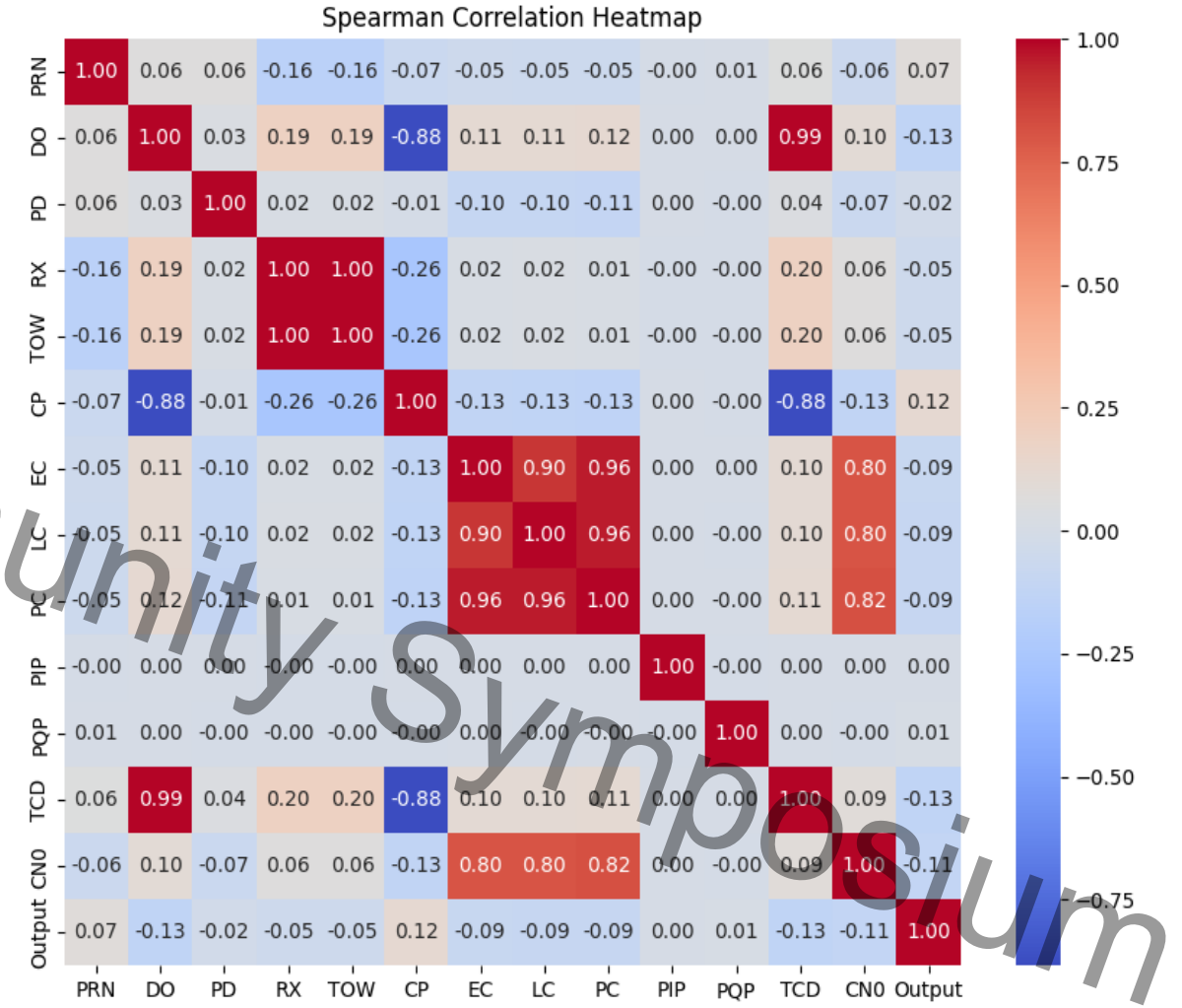
Feature Filtering using Spearman's Correlation

Feature Selection Filtering

Feature correlation using Spearman's Correlation

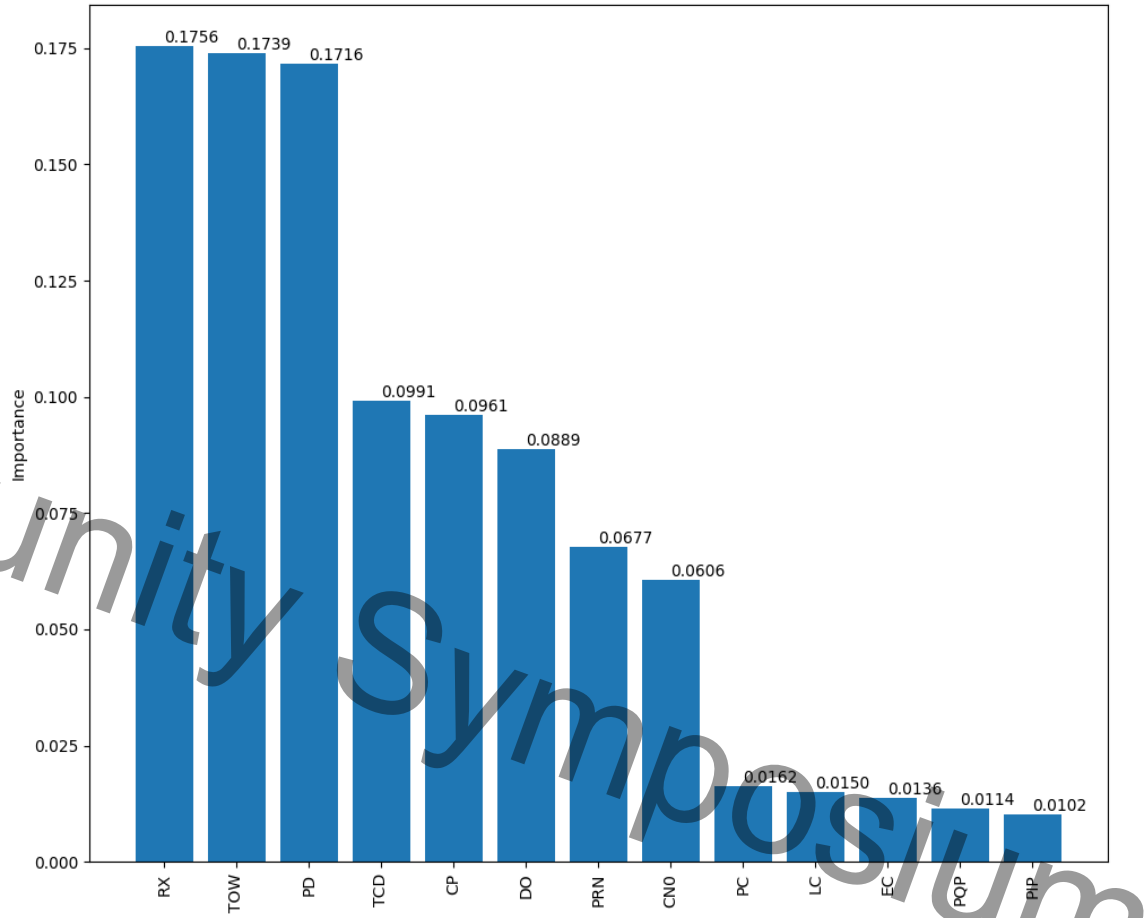
Highly correlated:

- (TCD, DO)
- (TOW, RX)
- (PC, EC)
- (PC, LC)
- (EC, LC)



Feature Filtering using Gini Index

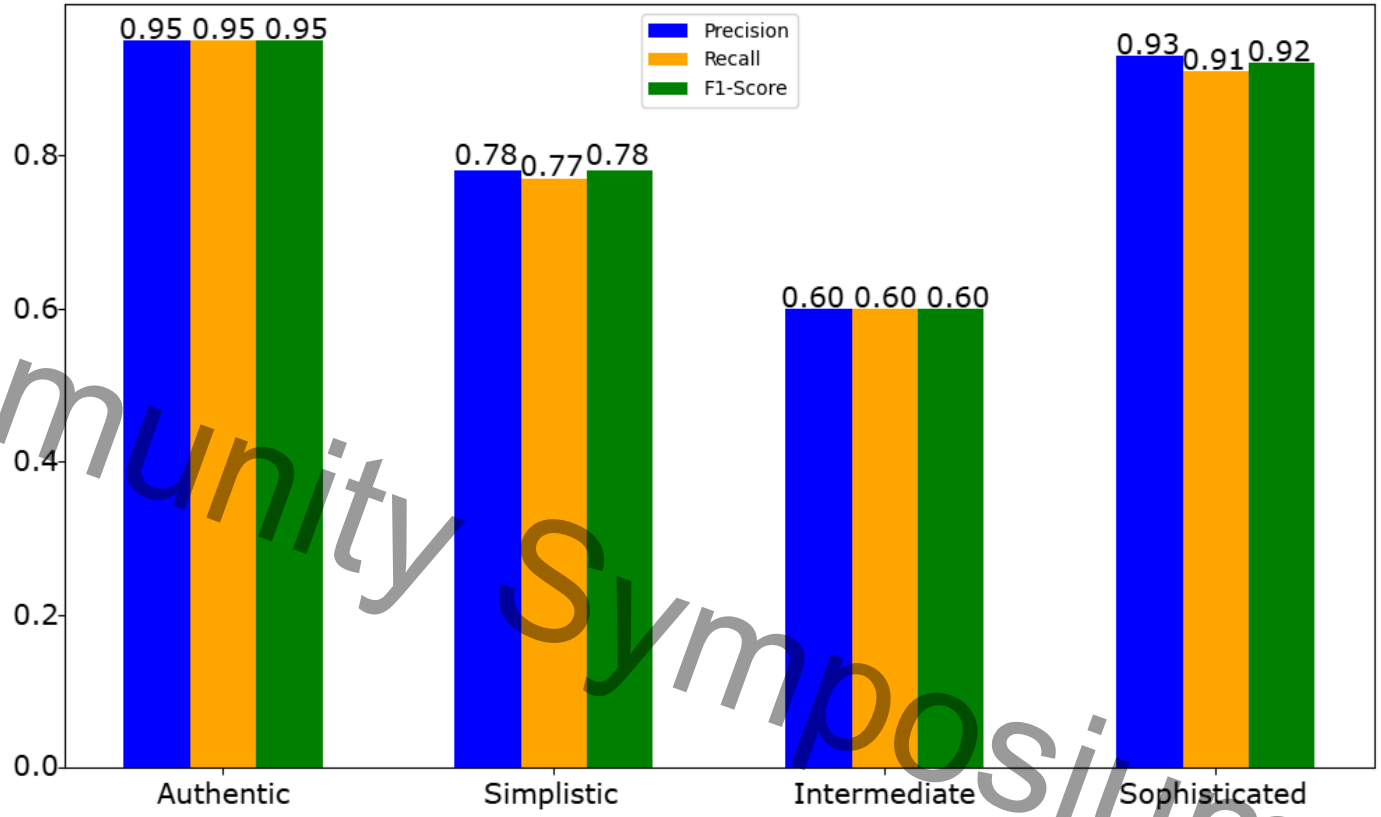
- Feature Importance Using Gini Index
  RX > TOW, TCD > DO, PC > LC, and PC > EC
- Removed the less important and highly correlated features: TOW, DO, LC, EC
- Selected Features: TCD, PRN, PD, RX, CP, PC, PIP, PQP, and C/N0



Results : Scenario 2

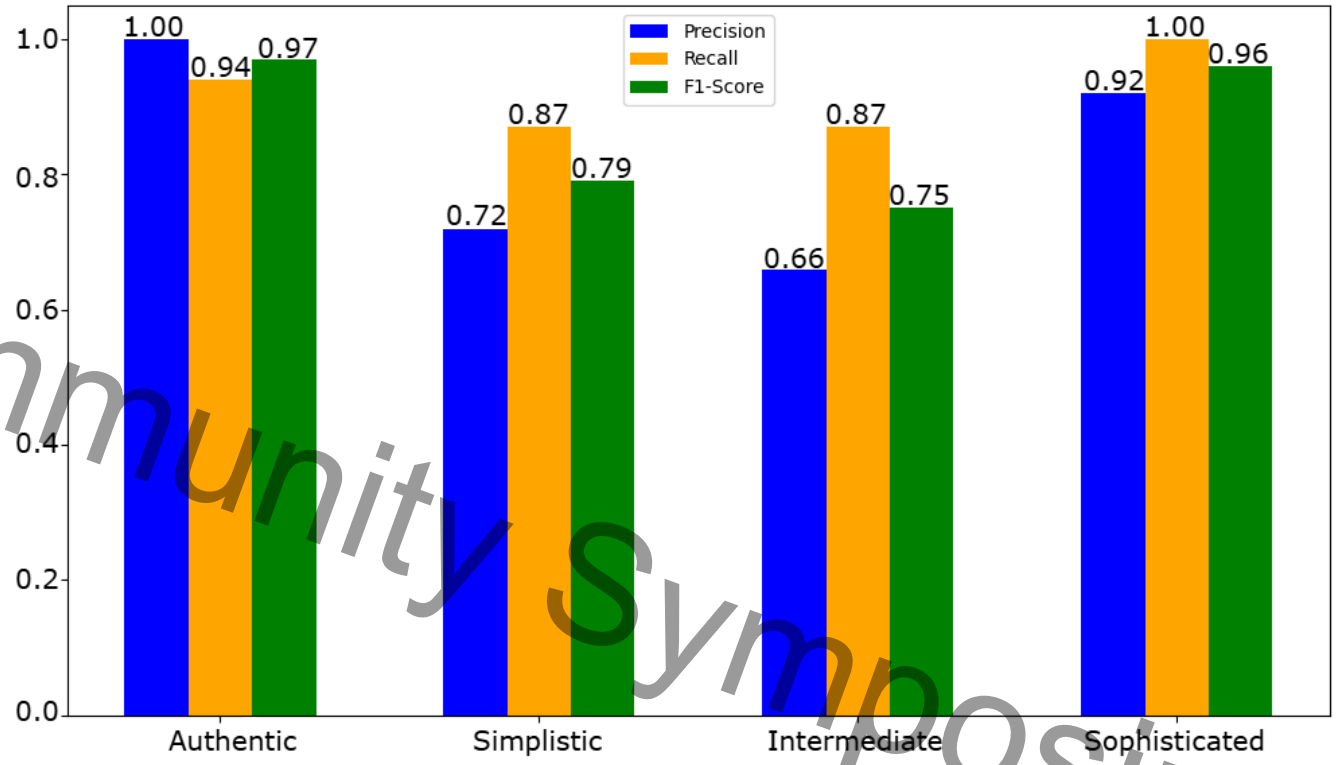
Was accurately able to distinguish authentic and sophisticated spoofed signals (>0.90)

Slightly improved performance in classifying simplistic (~0.77) and intermediate spoofed signals (~0.60)



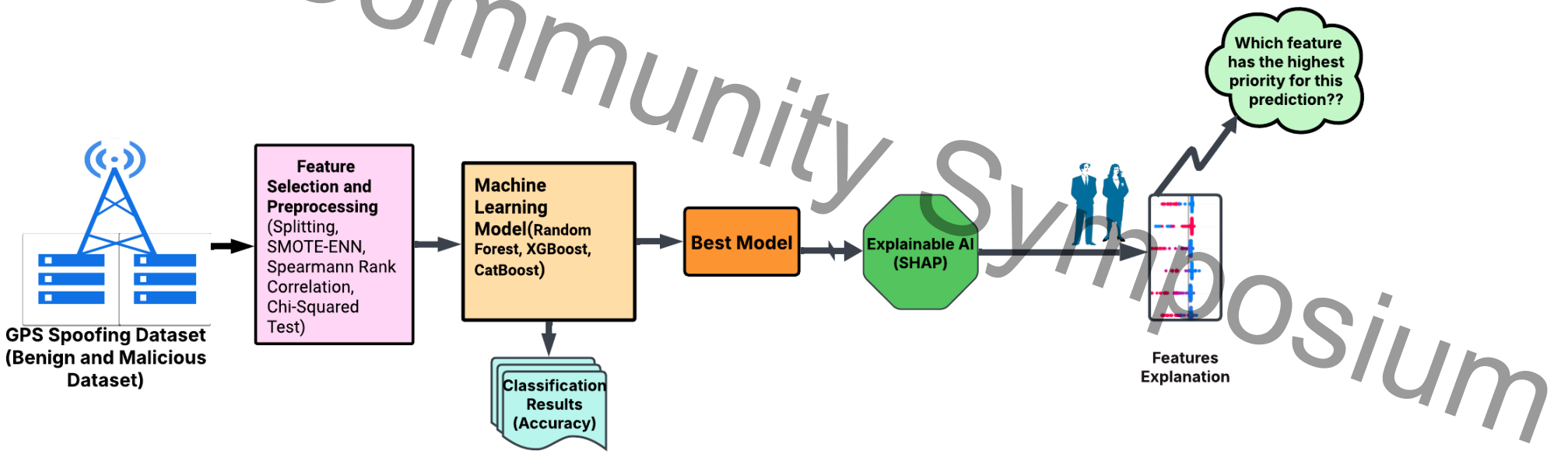
Results: Scenario 3

- Improved classification of authentic and sophisticated signals (>0.95)
- Greatly improved metrics for simplistic and intermediate signals



Explainability of GPS Spoofing Results

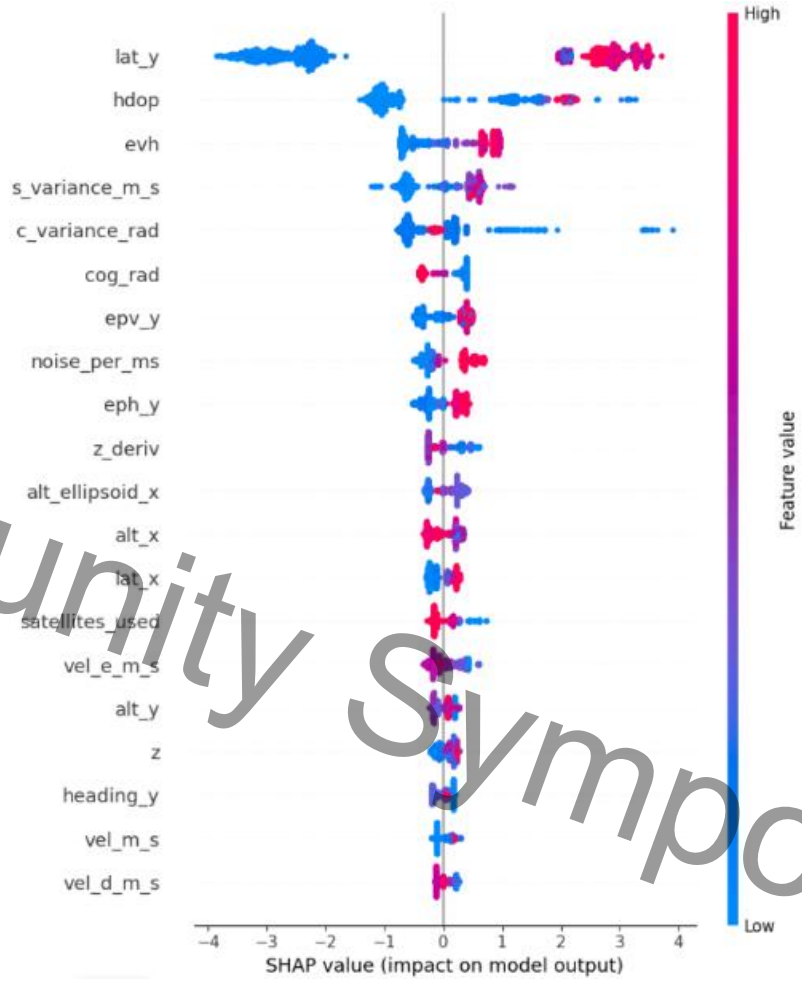
- Is the performance of ML model trust-worthy?
- Which features contribute the most for the prediction of the performance of the ML model?



Explainability of GPS Spoofing Results

Classifier	Hyperparameters	Accuracy (%)
XGBoost	n_estimators=50, max_depth=10, learning_rate=0.1, cv=5-fold	99.89
Random Forest (RF)	n_estimators=50, min_samples_split=10, min_samples_leaf=1, max_features=sqrt, max_depth=None	99.86
CatBoost	iterations=100, leaf_estimation_iterations=5, learning_rate=0.2, depth=6	99.87
LightGBM	metric=binary_logloss, learning_rate=0.05, feature_fraction=0.9, bagging_fraction=0.8, bagging_freq=5, objective=binary	99.87

Extracted Feature	Short term
hdop	Horizontal dilution of precision ;Higher HDOP, lower the accuracy [37].
lat_y	cordinates(y axis position); Sudden changes in latitude may indicate errors.
evh	Elapsed Vehicle Hour; low EVH may indicate poor routing.
s_variance_m_s	Speed variance; may have speed fluctuation due to spoofing.
c_variance_rad	change in direction variance.
cog_rad	Course over ground in radians;direction of movement inconsistency .
epv_y	Vertical position error in y axis.
noise_per_ms	Signal noise per millisecond.
eph_y	Horizontal position error (y axis).
z_deriv	Change in altitude over time
alt_ellipsoid	Altitude in 1E-3 above ellipsoid model(in millimeters).
alt_x	Altitude measurement; altitude measurement may altered by spoofing.
lat_x	latitude coordinate measurement; variation may cause by spoofing.
satellites_used	Number of satellites used for positioning; few satellites may have poor accuracy.
vel_e_m_s	GPS velocity in east direction; unusual speed may have spoofing.
alt_y	Measurement of altitude in y axis.
z	general altitude measurement
heading_y	direction of movement on the y -axis; Inconsistent heading may have spoofing
vel_m_s	GPS ground speed.
vel_d_m_s	GPS Down velocity; large downward speeds manipulated signals.



Gap in GPS Spoofing Detection

Human factors aspect is often neglected, even though pilots are the integral part of aircraft operation and control!

Studying Pilot Reaction to GPS Spoofing

Current CARS Flight Deck Equipment Benches

Basic aircraft scenario using typical patch antenna.
Center for Aerospace Resilient Systems (CARS) fight deck test bench during a GPS spoofing experiment (1).

3D position dynamically simulated via GPS/Galileo positional simulators (4).
Multi-leg waypoint paths, SV modeling, SBAS for WAAS/EGNOS.

Off-the-shelf King Air 200 and Citation Jet XLS avionics (1,3,7).
"Real" signal from first GPS simulator while a spoofed signal is generated on a second.

Both signals are combined and fed to both GPS antennas on the aircraft. (2, 5).

EMBRY-RIDDLE Aeronautical University

CENTER for AEROSPACE RESILIENT SYSTEMS

CyBASE CYBERSECURITY

ACI Cyber Rodeo & CTF, Daytona Beach Campus

Capture The Flag Competition: Government / Industry / Students & Faculty

Conclusion

- Machine Learning algorithms such as random forest and CatBoost are effective tools for spoofing detection
  - Provide approx. 99.89 % spoofing detection accuracy
- The result shows lat y, hdop, and evh are considered the three most important features having significant impact on model's prediction
- Additionally, pilot training is a critical aspect of mitigating GPS spoofing, as it enhances the ability to recognize and respond to spoofing attempts