Advanced GPS Signal Integrity Verification Using Neural Network Anomaly Detection

[1]Singam Aruna, [2]Kethavathu Srinivasa Naik, [3]Sirisolla Rama Devi, [4]Davala Swapna, [4]Mycherla Hakshaya, [4]Patnaikuni Siri Keerthika, [4]Chinthapalli Sravanthi, [4]Dalli Sravika, [4]Sontyana Lakshmi Tulasi

[1]Head of Department (M.Tech, Ph.D), [2]Professor, [3]Assistant Professor (M. Tech, Ph.D), [4]BTech Student

[1,3,4]Department of Electronics and Communication Engineering, Andhra University College of Engineering for Women, Visakhapatnam 530 017, India

[2]Department of Electronics and Communication Engineering, Vignan's Institute of Information Technology, Duvvada, Visakhapatnam 530 046, India

[4]swapnadavala95@gmail.com

***Abstract*—Modern navigation systems based on satellites become vulnerable to attacks when attackers transmit bogus signals to misguide systems about their position. A detection system for GPS spoofing attacks during real-time operations uses a dual algorithm composed of Random Forest and Artificial Neural Networks (ANN). The training process requires the algorithm to operate on simulated GPS-SDR-SIM software data containing vital measurement elements such as pseudorange together with carrier phase measurements along with Doppler shift parameters. Once features are extracted and normalized the Random Forest classifier operates first which leads to a 98.88% final detection accuracy through refinement in a two-hidden-layer neural network. The developed Flask-based web application enables both individual inputs using a form and bulk import through file upload functionalities for analysis execution. The system presents real-time voice and email notifications about spoofed signals to users for building their awareness. Experimental tests prove the system's high reliability standard while establishing its viable application scenario for defense purposes and transportation sites and financial network implementations.**

***Index Terms*—Flask Web Application, GPS Spoofing, Machine Learning, Neural Networks, Random Forest, Real-Time Detection.**

I. Introduction

When we examine the current interconnected world we see the Global Positioning System (GPS) provides basic functions for sector-wide navigation and communication and security operations. GPS receivers face growing dangers from spoofing attacks because counterfeit signals trick the receivers into delivering incorrect position data. The implementation of GPS spoofing attacks creates critical dangers that risk transportation safety and military operations and all forms of vital infrastructure. The detection methods currently in use fail to offer reliable spoofing detection because they depend too much on hardware systems and operational control factors.

This research work recommends a real-time GPS spoofing detection framework which unites Artificial Neural Networks (ANN) methodologies. The system operates efficiently with precise GPS signal parameter evaluation of Pseudorange and Carrier Phase and Doppler Shift which can be calibrated through training sessions. A Flask-based web interface operational at low cost provides real-time monitoring which automatically generates alerts because intelligent software detection methods can effectively secure systems that utilize GPS against advancing spoofing attacks.

II. Literature Review

Tremendous threats exist against GPS receivers because they suffer from growing intentional interference through jamming and spoofing methods. Spoofing attacks present the primary danger to receive pieces of equipment through deceptive signal manipulation, which bypasses detection methods, making them especially threatening [1].

Several approaches have been proposed to detect and mitigate GPS spoofing attacks, including machine learning (ML) and deep learning (DL) methods [2]. Spoofed signals typically exhibit extra delay and higher power than genuine ones, affecting parameters such as pseudorange, carrier phase, and Doppler shift [3]. Spoofing involves broadcasting counterfeit signals that mislead or disrupt receiver operations [4]. Filtering techniques have been suggested to eliminate outliers; however, they require a majority of authentic signals to remain effective [5].

Recent studies explored artificial neural networks (ANNs) to classify spoofed signals based on metrics like signal-to-noise ratio and pseudorange, yet comprehensive post-detection defense mechanisms are still lacking [6]. Supervised and unsupervised models have been assessed across accuracy and detection time, with decision tree classifiers often outperforming others [7].

III. Materials

Programming Language: Python 3.9

Machine Learning Framework: The detection system uses TensorFlow for model development and inference processes, Keras to develop neural networks, and Scikit-learn to process and evaluate data.

Signal Simulation Tool: GPS-SDR-SIM serves as an open-source software-defined radio system signal simulator.

Broadcast Ephemeris Data (BRDC File) is a RINEX navigation file obtained from the official GPS archive that serves to reproduce satellite signal movements when performing spoofing attacks.

Data Analysis Libraries: NumPy, Pandas, and Matplotlib.

Development Environment: Jupyter Notebook.

Web Technologies: The web interface for spoofing detection operates through Flask as well as HTML, CSS and JavaScript.

IV. METHODOLOGY

Dataset Generation

A GPS spoofing dataset was created through authentic signal generation and spoofed signal creation followed by crucial signal features extraction for classification use. The development of authentic signals occurred through GPS-SDR-SIM software which utilized broadcast ephemeris files retrieved from the IGS repository (e.g., brdc0040.25n). The generated GPS signals from .\gps-sdr-sim -e brdc0040.25n -b 8 -d 60 -l 17.686836,83.218475,45 -o gps_authentic.bin ran for 60 seconds with 8-bit depth resolution at specified coordinates. The signals were spoofed when different locations got specified for generation. The system extracted three features which included Doppler Shift and Carrier Phase and Pseudorange. The conversion of binary files to CSV format enabled the collection of 2000 samples from authentic and spoofed classes to create a total dataset of 4000 labeled samples. Label 1: Authentic GPS signals , Label 0: Spoofed GPS signals.

This dataset is used as the training and evaluation source for machine learning models for GPS spoofing detection.

Performance Evaluation of the Four Algorithms used

The evaluation included an SVM alongside Logistic Regression, XGBoost, and Random Forest as the key machine learning algorithms. Recorded accuracy values exist for each model during testing.

Different algorithms used in the project are compared through Table 1.

TABLE 1 Comparison of Different Algorithms

Model	Accuracy	Precision	Recall	F1-Score
Random Forest	0.9888	0.9889	0.9888	0.9888
Support Vector Machine	0.9750	0.9760	0.9750	0.9750
XGBoost	0.9900	0.9901	0.9900	0.9900
Logistic Regression	0.9363	0.9438	0.9363	0.9362
Hybrid NN	0.9888	0.9889	0.9888	0.9888

The SVM model reached 97% accuracy because it diagnosed data structure patterns successfully, although it had an increased risk of overfitting.

The logistic regression algorithm reached 93% accuracy, although it provided a clear interpretation while yielding less precise results during boundary detection.

XGBoost delivered superior performance compared to each model individually by reaching 99% accuracy because of its ensemble mechanism that made it resistant to overfitting.

The test data validated the effectiveness of XGBoost classifiers as they reached high GPS spoofing detection accuracy through trained engineered features.

Deep Learning Model Training

Training and Evaluation Process: The dataset is split into 80% training and 20% testing. Training is conducted over 100 epochs with a batch size of 16. The model checks its validation data performance after each epoch run to optimize weight adjustments for enhanced accuracy. The system tracks development through performance measures, including accuracy rates, together with loss metrics.

V. EXPERIMENTAL DETAILS

System Development & Deployment

A. Flask-Based Web Application

Real-time GPS spoofing detection runs through a Flask-based web application that enables users to input GPS parameters using an HTML/CSS/JavaScript interface for displaying authenticity results in a dynamic format.

B. Security Enhancement

The system integrates an alert mechanism that operates in real time to enhance GPS spoofing attack security. The user submits GPS signal parameters as depicted in Fig.1. The System processes the data and classifies it as Authentic GPS Signal or Spoofed GPS Signal using Machine Learning & Deep Learning models. If spoofing is detected, an Email Alert is triggered. The system provides Real-time Results through a Flask-based web application.

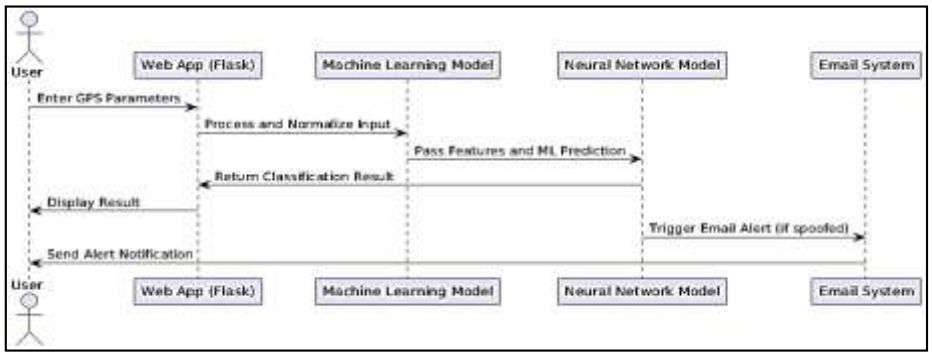

Fig. 1 — Sequence Diagram

VI. Experimental Evaluation

The Neural Network Architecture contains One Hidden Layer with 16 and 20 neurons and Two Hidden Layers with 16 (8-8 split) and 20 (10-10 split) neurons.

A. Confusion Matrix

Obained Values: The classification results demonstrate solid results showing high numbers of accurate predictions along with minimal numbers of incorrect predictions.

$$C = \begin{pmatrix} 376 & 2 \\ 7 & 415 \end{pmatrix}$$

B. Performance Analysis

By expanding the number of neurons the proposed system improves its ability to detect both authentic and spoofed voice samples while increasing accuracy in classifying them and decreasing incorrect and missing detections and false alarms. The recognition system performs better with 20 neurons than with 16 neurons in single-layer as well as two-layer configurations. Additional layers contribute to better spoofed alarm control without sacrificing accuracy performance. The number of neurons in a network enables enhanced detection capabilities by deepening the performance boundaries between models with one or two layers. Classification results improve through the combination of two hidden layers which maximizes Pad and Psd values thus achieving better classification outcomes and simultaneously reduces false negatives by minimizing Pmd values because of the network depth. The system reliability becomes better with low Pfa values in both hidden layers that prevent false signals from classifying genuine GPS signals and enhance the overall usability as shown in Table 2.

TABLE 2 Performance Analysis of Hidden Layers

Layers/Neurons	Pcc (%)	Pmc (%)	Psd (%)	Pad (%)	Pmd (%)	Pfa (%)
One Hidden/16	98.4	1.6	99.1	97.7	0.9	2.3
Two Hidden/16	98.8	1.2	99.5	98.1	0.6	2.0
One Hidden/20	98.7	1.3	99.3	98.0	0.7	2.0
Two Hidden/20	99.0	1.0	99.8	98.3	0.4	1.7

C.Classification Report

According to Table 3 both the spoofed signal detection accuracy was 98% and the identification of authentic signals reached 100% F1-score at 0.99. Recall performance acts as a tool to decrease spoofing detection failures, thus improving system sensitivity. A reliable and accurate system emerges from the F1-score because it ensures an optimal balance between the detection of false alarms and missed signals.

- The spoofing detection system in our project attains improved performance through optimized precision and recall ratings and F1-score measurement.
- By using precision, the system decreases wrong alarms, allowing it to predict spoofed signals with greater accuracy.
- Since overall accuracy, as shown in Table 3, is 99%, Precision ensures that our project has fewer false alarms, recall ensures fewer missed spoofed signals, and the F1-score balances both.

TABLE 3 Classification Report Showing Overall Accuracy

Class	Precision	Recall	F1-score	Support
Spoofed	0.98	1.00	0.99	378
Authentic	1.00	0.98	0.99	422
Overall Accuracy	99%	NA	NA	NA

VII. Results and Discussion

A. Visualizations

Our project utilizes three features whose importance appears in Fig.2. The evaluation of GPS signal parameter contributions to spoofing detection required training a Random Forest classifier with labeled data. The trained model showed that Carrier Phase represents the highest influence among features with a score of 0.55 while Doppler Shift received a score of 0.3 followed by Pseudorange at 0.13.

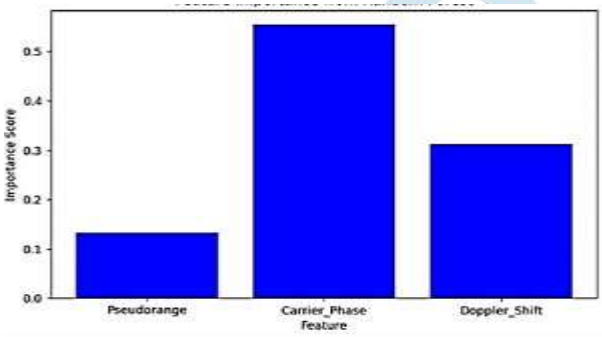

Fig. 2 — Feature Importance

In this research paper we analyzed feedforward network capability using one and two hidden layers at different neuron configurations for precision detection and false alarm and missed detection rates.

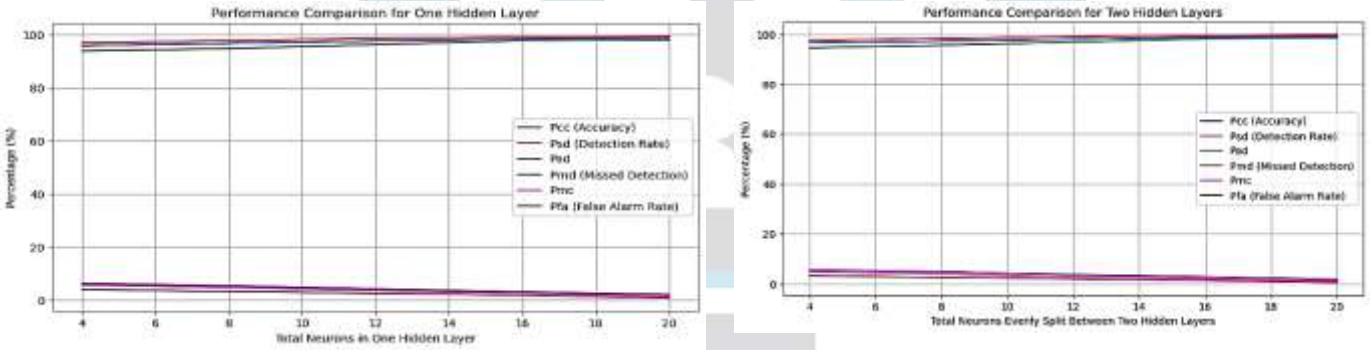

Fig. 3 — Model Performance vs Neuron Count

Figure 3(a): Performance Comparison for One Hidden Layer. Figure3(b): Performance Comparison for Two Hidden Layers

As per Fig. 3 (a), (b), we can say that the Psd (spoofing detection rate) and Pad (attack detection rate) are higher in two hidden layers. Pmd (missed detections) is lower for two hidden layers, meaning fewer spoofing attempts go undetected. Pfa (false alarm rate) is lower for two hidden layers, making the system more reliable. Therefore, the simulation results demonstrate that using two hidden layers provides better GPS spoofing detection performance.

B. Training vs Validation Accuracy

Training Accuracy: The model achieves nearly 100% accuracy. Fig. 4 illustrates how the model achieves almost complete accuracy when trained with the given data, indicating successful pattern learning. The model shows reliable generalization for unseen data through its stable validation accuracy of 99% throughout all epochs.

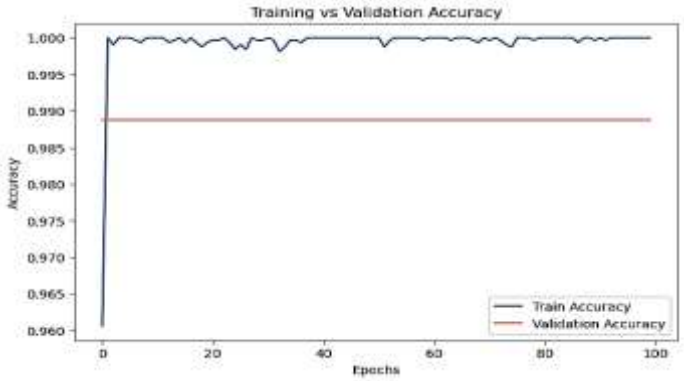

Fig. 4 — Comparison between Training and Validation Accuracy

C. System Output

The web application, designed using Flask, was created in Visual Studio and was capable of demonstrating a functioning web application that produced GPS spoofing detection. A user could input GPS parameters into the modern web interface. The resulting output was checked using three cases. The three cases included the uploaded authenticated dataset and one of the uploaded spoofed datasets to analyze the number spoofed signals from the dataset as shown in Fig.5 (a). The analysis output was also downloadable as shown in Fig.5 (b) and generated additional reports, which provided additional analysis.

Figure 5(a): Model output identifying entered values as spoofed GPS signals. Figure 5(b): Results for the uploaded CSV file.

In Fig.6, an email alert is sent to the receiver's email address when a spoofed signal is detected.

Fig. 6 — Email interface displaying alert message for spoofing event detection

The model requires well-quality training data, including various samples to achieve effective performance results. Experimental findings establish that complicated machine learning methods create reliable systems to detect GPS spoofing behavior.

VIII. Conclusion and Future Work

The research introduces a dependable system that detects GPS spoofing in real time to maintain navigation system security. The study used GPS-SDR-SIM to develop simulations of authentic and spoofed signals, which automatically collected Doppler shift together with carrier phase and pseudo-range patterns for anomaly detection purposes. Neural networks functioning inside a machine learning-based classifier could adjust its detection performance to natural signal irregularities to enhance accuracy.

Practical deployment received support through the development of a user-friendly Flask interface, which incorporated real-time alerts and voice alarm notifications delivered through an SMTP server. Among industrial applications this system provides exceptional performance during autonomous navigation operations and secure communication network operations. The project will advance through future development stages by expanding its features, integrating big real-world data sources and implementing blockchain systems for authenticating GPS signal reliability.

IX. Acknowledgment

This research work received guidance from Dr. K. Srinivasa Naik at Vignan's Institute of Information Technology. The authors thank Dr. Aruna, the Department Head of Electronics and Communication Engineering, and Dr. Rama Devi from AUCE for Women for their instrumental support and motivation.

References

[1] J. M. Jahantab, S. Tohidi, M. R. Mosavi, and A. Ayatollahi, "GPS spoofing detection using CAF images and neural networks based on proposed peak mapping dimensionality reduction algorithm and TCNN model," 4 December 2024.
[2] S. C. Bose, "GPS spoofing detection by neural network machine learning," 20 December 2021.
[3] M. Jones, "Spoofing in the Black Sea: What happened?" 11 October 2017.
[4] H. Niedermeier, H. Beckmann, and B. Eissfeller, "Robust secure and precise vehicle navigation system for harsh GNSS signal conditions," in Proc. 2013 Int. Conf. on Localization and GNSS (ICL-GNSS), June 2013.
[5] M. L. Psiaki and T. E. Humphreys, "GNSS spoofing and detection," June 2016.
[6] R. A. Agyapong, M. Nabil, A. R. Nuhu, M. I. Rasul, and H. Homaifar, "Efficient detection of GPS spoofing attacks on unmanned aerial vehicles using deep learning," December 2021.
[7] K. Radoš, M. Brkić, and D. Begušić, "Recent advances on jamming and spoofing detection in GNSS," 28 June 2024.
[8] International GNSS Service, "Daily data archive," Available: https://igs.org/data/#daily_data, accessed January 2025.