An Interpretable Ensemble Learning Method for GPS Spoofing Detection with Feature Selection

Tengtuo Chen , Qi Shao , Guibin Peng * , Shuo Li * , Haotian Zhong , Jianchun Zhang , Shunkun Yang

Posted Date: 16 April 2026

doi: 10.20944/preprints202604.1124.v1

Keywords: GPS spoofing detection; ensemble learning; interpretability; transformer; feature selection

 doi:10.20944/preprints202604.1124.v1

Article

An Interpretable Ensemble Learning Method for GPS Spoofing Detection with Feature Selection

Tengtuo Chen [1], Qi Shao [1], Guibin Peng [1,*], Shuo Li [1,*], Haotian Zhong [1], Jianchun Zhang [2] and Shunkun Yang [3]

[1] COMAC Beijing Aircraft Technology Research Institute, Beijing 102211, China
[2] Hangzhou Innovation Institute, Beihang University, Beijing 310052, China
[3] School of Reliability and Systems Engineering, Beihang University, Beijing 100191, China
* Correspondence: pengguibin@comac.cc (G.P.); lishuo@comac.cc (S.L.)

Abstract

Global Positioning System (GPS) spoofing poses severe threats to navigation safety, necessitating robust detection mechanisms with enhanced interpretability. This study proposes Stack-TabNet, a novel stacked ensemble learning framework integrating XGBoost, Random Forest, and the attentive transformer-based TabNet network. To address model opacity, an interpretable feature attribution mechanism is employed to quantify feature contributions and guide optimization. Experiments are conducted on a complex dataset comprising authentic and spoofed GPS signals across four classes, characterized by high-dimensional signal metrics and severe class imbalance. The initial model utilizing all available features demonstrates robust detection capability. Subsequently, an optimized variant utilizes a subset of top-ranked features identified by the interpretation mechanism, yielding further improved accuracy. Comparative analysis confirms that the proposed framework surpasses all traditional machine learning and deep learning baselines. The analysis identifies Pseudorange and Time of Code Delay as the most discriminative features. These results indicate that combining ensemble learning with interpretable feature selection significantly enhances detection accuracy and training efficiency for GPS anti-spoofing applications.

Keywords: GPS spoofing detection; ensemble learning; interpretability; transformer; feature selection

1. Introduction

GPS has become an indispensable component of modern navigation infrastructure, serving critical applications across civil aviation, unmanned aerial systems (UAS), autonomous maritime vessels, and consumer mobile devices [1–3]. The reliability and integrity of GPS-derived positioning information are paramount, as spoofing attacks that manipulate authentic satellite signals can induce catastrophic consequences, including aircraft misnavigation, unauthorized drone diversion, and maritime collision incidents. Consequently, the development of robust GPS spoofing detection mechanisms has emerged as a research priority of substantial significance within the remote sensing and navigation communities. This research domain has attracted considerable scholarly attention in recent years, with numerous methodological advances documented in the literature [4]. The practical applicability of effective anti-spoofing solutions is widely recognized, given their potential deployment across safety-critical transportation systems. Furthermore, GPS signal authentication and anomaly detection constitute an increasingly established research paradigm, supported by both theoretical frameworks and empirical validations.

As illustrated in Figure 1, GPS positioning fundamentally relies on the simultaneous reception of signals from multiple satellites (typically four or more), whereby the receiver calculates its three-dimensional position through trilateration based on signal propagation time measurements [5–8]. In a spoofing attack scenario, an adversarial transmitter deliberately broadcasts counterfeit GPS signals that

 doi:10.20944/preprints202604.1124.v1

mimic authentic satellite transmissions, thereby deceiving the target receiver into computing erroneous position, velocity, and time solutions. The spoofer, as depicted in the Figure 1, emits malicious signals (represented by red dashed lines) that compete with or overwhelm legitimate satellite signals (represented by blue solid lines) received by the aircraft. Such attacks can be categorized into simplistic, intermediate, and sophisticated variants, distinguished by their signal generation complexity and synchronization accuracy with authentic satellite constellations.

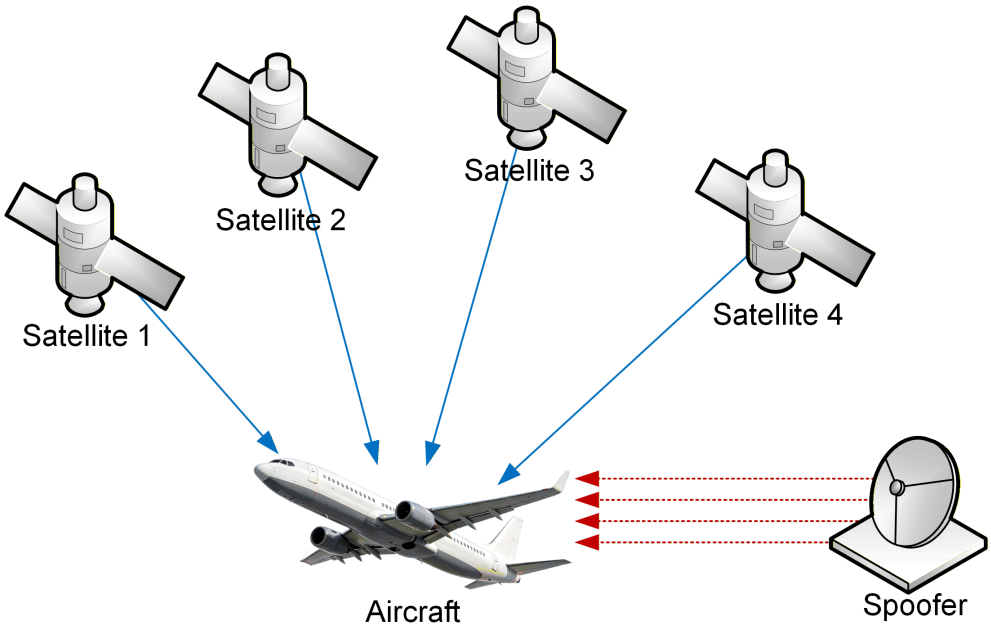


Figure 1. GPS Positioning and Spoofing. A typical example of an aircraft being spoofed: the solid blue line represents the actual GPS signal, while the dashed red line represents the fake signal transmitted by the spoofer.

1.1. Related Work

To address the vulnerability of GPS signals to spoofing interference, extensive research efforts have been undertaken, encompassing signal processing-based techniques, machine learning classifiers, and hybrid detection frameworks. Previous investigations have demonstrated the efficacy of various approaches, including power monitoring, signal quality metrics, cryptographic authentication, and data-driven anomaly detection methodologies.

1.1.1. Signal Processing-Based Techniques

In the domain of signal processing-based techniques, Fan et al. [9] propose a spoofing matching algorithm to identify GPS deception. Numerical simulations are conducted within test scenarios, demonstrating the effective identification of Global Spoofing Attack (GSA) locations and the recovery of GPS pseudo-synchronous phasor data, which subsequently refines GPS state estimation results. Kwon et al. [10] leverage accelerometers within an Attitude and Heading Reference System (AHRS) to directly detect GPS spoofing interference. The detection performance of this approach is analyzed using corresponding Probability Density Functions (PDFs), wherein the magnitude of acceleration error serves as the decision variable for calculating the probability of spoofing. Basan et al. [11] design a spoofing detection methodology utilizing Kullback–Leibler divergence, integrated with essential analytical parameters and data normalization. This strategy mitigates the reliance on extensive prior data, a common constraint in traditional detection schemes.

1.1.2. Machine Learning-Based Classifiers

Within the sphere of machine learning, advancements in semantic segmentation [12], multi-class classification [13], and ensemble learning [14] have significantly propelled the development of GPS spoofing detection. For instance, Wei et al. [15] selected specific flight data types—encompassing

 doi:10.20944/preprints202604.1124.v1

altitude and horizontal position control processes—as feature inputs. Multiple algorithms are employed to train and generate CONSTDET, a classifier tailored for GPS spoofing attacks. Bose and Sam [16] adopt supervised machine learning techniques, utilizing GPS observable features such as pseudorange, carrier phase, Doppler shift, and carrier-to-noise density ratio (C/N_0) to discriminate between authentic and forged signals. Comprehensive investigations are performed regarding network architecture, training sample size, the number of hidden layers, neuron distribution across layers, and the total count of hidden neurons. Acknowledging that conventional machine learning methods often exceed the computational constraints of small UAVs, Ren et al. [17] propose a lightweight detection model based on Long Short-Term Memory (LSTM) networks deployed at the ground control station. Through knowledge distillation, this model is compressed into a parameter-efficient variant capable of operating within UAV onboard control systems, with experimental results validating its feasibility.

1.1.3. Hybrid Detection Frameworks

In the context of hybrid detection frameworks, Meng et al. [18] address GPS attacks targeting UAV swarms by combining swarm collaborative positioning with a security machine optimal marking mechanism, yielding a detection method characterized by high real-time performance. Song et al. [19] introduce a hybrid spoofing detection approach that fuses Temporal Convolutional Networks (TCN) with Kalman Filters. This integration alleviates Inertial Navigation System (INS) error drift and generates virtual GPS trajectories, thereby establishing correlations across continuous time windows. Consequently, the mechanistic capabilities of INS-aided GPS spoofing detection are enhanced, and challenges related to strain positioning in GPS signal reconstruction are resolved. Meanwhile, observer-based hybrid diagnosis methods [20] can also be employed in GPS attacks detection. Furthermore, Kuriş et al. [21] contribute to the comparative analysis of hybrid methodologies by providing a detailed performance evaluation of LSTM, Gated Recurrent Unit (GRU), and hybrid LSTM–GRU deep learning models applied to GPS spoofing attack detection.

1.2. The Gap in the Literature and the Contribution of This Study

However, existing detection methods frequently exhibit limitations in generalization capability across diverse attack scenarios and operational environments, while the interpretability of deep learning-based detectors remains insufficiently explored. These gaps motivate the extension of current methodologies through ensemble learning architectures that integrate complementary model strengths with explainable artificial intelligence principles.

Overall, in this paper, we develop a robust ensemble learning framework for GPS spoofing detection, integrating deep learning attention mechanisms with interpretable feature selection. The following three aspects describe the primary contributions of this study.

(1) A novel stacked ensemble learning framework tailored for GPS spoofing detection is proposed. Considering the complexity of signal features in spoofing scenarios, we integrate the attention-based TabNet network with traditional tree-based models within a stacking architecture. The newly proposed Stack-TabNet model dramatically improves the detection robustness and saves computing resources compared to standalone deep learning models. Therefore, our proposed ensemble method has significant performance improvement compared with traditional machine learning methods.

(2) We introduce a comprehensive interpretability analysis for GPS spoofing detection models. For the first time in this context, we employ SHapley Additive exPlanations (SHAP) to decode the decision-making process of the TabNet-based ensemble. A total of 13 signal features are analyzed, which can be used to study the physical characteristics distinguishing spoofed signals from authentic ones. It is worth mentioning that the interpretability analysis is conducted in real-world navigation scenarios, which is a challenging process due to the high dimensionality of signal data. In addition, visualizing feature contributions is a critical task due to the safety-critical nature of aviation navigation systems.

 doi:10.20944/preprints202604.1124.v1

(3) Through SHAP-guided feature selection, a refined detection variant is developed to reduce model complexity and improve computational efficiency. By retaining only the most informative features, the training process becomes less dependent on high-dimensional inputs, which is particularly advantageous for real-time GPS monitoring applications. Experimental results demonstrate that our optimized method named Stack-TabNet-2 can improve the classification accuracy of the full-feature model with only the top 8 features and can exceed the classification effect of traditional supervised learning baselines while minimizing computational overhead.

The remainder of this paper is organized as follows: Section 2 presents dataset and proposed methodology in detail. Section 3 reports experimental results and comparative analyses. Section 4 discusses the implications and limitations of this work. Finally, Section 5 concludes the paper and outlines future research directions.

2. Materials and Methods

The systematic workflow for the proposed GPS spoofing detection methodology is illustrated in Figure 2. The research pipeline is partitioned into four primary functional modules, which facilitate a transition from raw signal acquisition to an optimized, interpretable detection architecture.

As depicted in Figure 2(a), the initial phase involves the acquisition of 13-dimensional GPS signal features and subsequent pre-processing. To address the inherent class imbalance between authentic and spoofed instances, an under-sampling strategy is executed to construct a balanced training environment across four categories: Authentic, Simplistic, Intermediate, and Sophisticated attacks.

The core modeling phase, designated as Stack-TabNet 1, is presented in Figure 2(b). This stage employs a multi-fold cross-validation training regime for three heterogeneous base learners. The generated class probabilities are then synthesized by a Logistic Regression meta-classifier. This initial ensemble serves as the baseline for high-performance detection across all available signal attributes.

Subsequently, a post-hoc interpretability analysis is performed as shown in Figure 2(c). SHAP values are computed to quantify the global and local contributions of each signal feature. This process decodes the "black-box" nature of the ensemble and identifies the most discriminative physical indicators of spoofing.

Finally, an optimized detection variant, Stack-TabNet 2, is derived in Figure 2(d). Guided by the SHAP-driven importance ranking, a feature selection policy is implemented to retain the top eight most influential features. This refined model is retrained to evaluate the feasibility of achieving superior detection accuracy with reduced computational overhead, thereby ensuring suitability for real-time navigation safeguards.

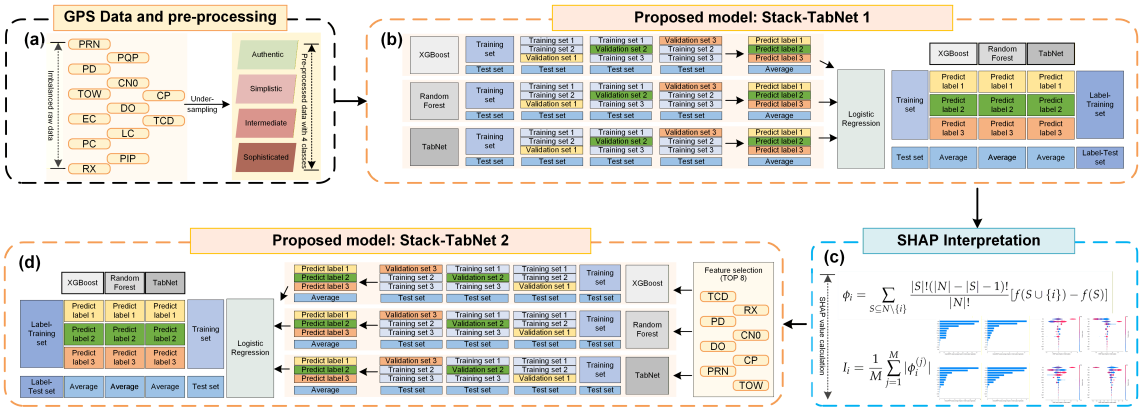


Figure 2. The overall research framework of the proposed GPS spoofing detection system.

2.1. Dataset Description and Preliminary Analysis

The empirical data utilized in this study comprises recordings of GPS intrusion incidents [22]. Authentic signal measurements are acquired via an eight-channel GPS receiver mounted on a ground

 doi:10.20944/preprints202604.1124.v1

vehicle. Velocity profiles varying from 0 to 60 mph are maintained to simulate UAS flight dynamics, while stationary observations are conducted at three distinct elevated locations to replicate hovering scenarios. Thirteen distinct signal parameters are derived from eight parallel processing channels during the acquisition phase. Beyond genuine transmissions, three categories of spoofing intrusions—classified as simplistic, intermediate, and sophisticated—are artificially generated to ensure comprehensive coverage of threat vectors.

The specific parameters extracted during signal processing are detailed in Table 1. These attributes encompass both navigation data and signal quality metrics, providing a multidimensional view of the receiver state.

The initial dataset exhibits a significant class imbalance, reflecting real-world operational conditions where authentic signals vastly outnumber attack instances. The distribution across the four target categories is recorded as follows: Class 0 (Authentic) contains 397,825 samples; Class 1 (Simplistic Attack) comprises 36,458 samples; Class 2 (Intermediate Attack) includes 44,232 samples; and Class 3 (Sophisticated Attack) consists of 32,015 samples. To mitigate the potential bias introduced by this disparity during model training, undersampling techniques are subsequently applied, as detailed in the EXPERIMENT section. The total number of observations amounts to 510,530 instances, each characterized by the thirteen dimensions outlined above.

Table 1. Description of the 13 extracted GPS signal features.

Feature	Description
PRN	Pseudo-Random Noise identifying the specific satellite source.
DO	Doppler Offset measuring frequency shift due to relative motion (Hz).
PD	Pseudorange estimating satellite-receiver distance based on travel time (m).
RX	Receiver Time recorded by the local hardware clock.
TOW	Time of Week indicating seconds elapsed since the GPS week start.
CP	Carrier Phase capturing accumulated phase difference (cycles).
EC	Early Correlation value used for code tracking loops.
LC	Late Correlation value utilized for code tracking loops.
PC	Prompt Correlation value employed for data demodulation.
PIP	Prompt I-Prompt representing the in-phase correlation component.
PQP	Prompt Q-Prompt representing the quadrature-phase correlation component.
TCD	Time of Code Delay between received and local code (s).
CN0	Carrier-to-Noise Density Ratio indicating signal strength (dB-Hz).

To investigate the inter-dependencies among the 13 extracted GPS signal features, a correlation matrix heatmap is constructed, as illustrated in Figure 3. The Pearson correlation coefficients are computed to quantify the linear relationships between each pair of features, with values ranging from -1 to $+1$.

Several notable correlation patterns are observed from the heatmap. First, the correlation-based features EC (Early Correlation), LC (Late Correlation), and PC (Prompt Correlation) exhibit strong positive correlations with each other (correlation coefficients $\approx 0.9 - 0.96$), which is expected given their shared origin in the signal correlation process. Second, DO (Doppler Offset) demonstrates strong negative correlations with CP (Carrier Phase) and TCD (Time of Code Delay) (correlation coefficients ≈ -0.82), reflecting the inverse relationship between frequency shift and phase/code measurements. Third, TCD and DO show near-perfect positive correlation, as both represent temporal information. Additionally, CN0 (Carrier-to-Noise Density Ratio) displays moderate positive correlations with EC, LC, and PC (correlation coefficients $\approx$ 0.75–0.78), indicating that signal strength influences correlation magnitudes.

The correlation analysis reveals that while some features are highly interdependent, most feature pairs exhibit weak correlations (coefficients < 0.3), suggesting that the 13-dimensional feature space captures complementary information for spoofing detection. This finding justifies the inclusion of all features in the initial model training. Furthermore, it indicates that the selection of training features

 doi:10.20944/preprints202604.1124.v1

significantly influences the final outcome, warranting a detailed investigation into feature importance and optimization in the subsequent sections.

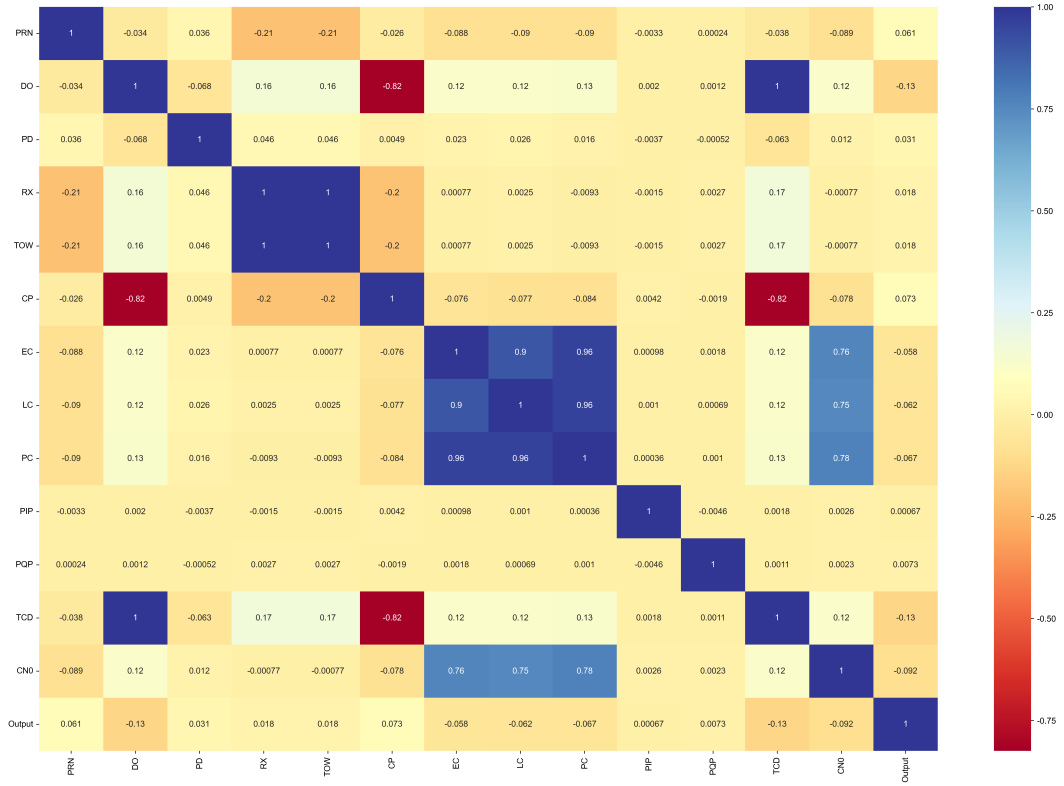


Figure 3. Correlation heatmap of the 13 GPS signal features. The color intensity represents the strength of Pearson correlation coefficients, with blue indicating positive correlation and red indicating negative correlation.

2.2. Stack-TabNet Ensemble Model

A novel heterogeneous ensemble framework, designated as Stack-TabNet, is constructed to enhance the robustness and interpretability of GPS spoofing detection. The architecture operates through a two-level hierarchy, wherein diverse base learners are aggregated by a meta-classifier. This design leverages the complementary strengths of deep learning attention mechanisms and traditional tree-based ensemble methods. The overall workflow of the proposed methodology is illustrated in Figure 4.

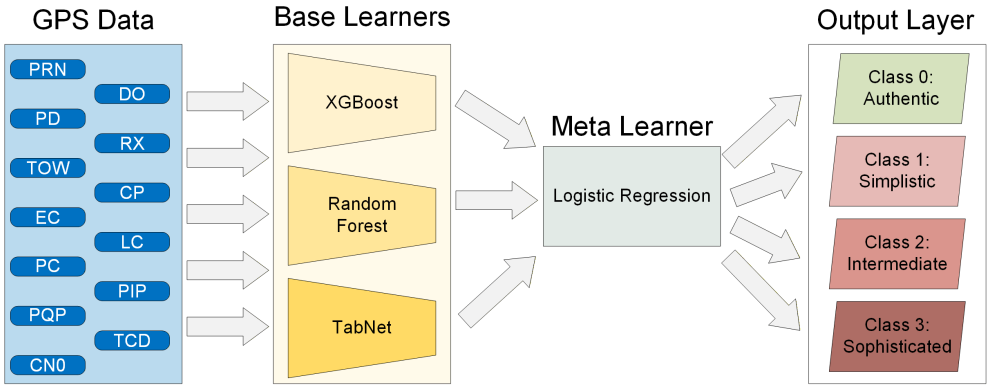


Figure 4. Architecture of the proposed Stack-TabNet ensemble model. The input layer consists of 13 GPS signal features. The first layer comprises three base learners: XGBoost, Random Forest, and TabNet. Their prediction probabilities, along with original features, are fed into the second layer meta-learner (Logistic Regression) for final classification.

 doi:10.20944/preprints202604.1124.v1

2.2.1. Base Learners Configuration

Three distinct algorithms are employed as base learners to ensure model diversity and complementary learning capabilities. The strategic selection of these classifiers is motivated by the hypothesis that their integration through stacking will yield superior detection performance compared to any individual base learner, a claim that is substantiated in the experimental results section.

First, XGBoost is utilized for its efficiency in handling structured tabular data through gradient boosting. The model constructs an ensemble of decision trees sequentially, where each tree corrects the residuals of its predecessors. The objective function is formulated as:

$$\mathcal{L} = \sum_{i=1}^{n} l(y_i, \hat{y}_i) + \sum_{k=1}^{K} \Omega(f_k) \tag{1}$$

where l denotes the loss function, $\hat{y}_i$ represents the predicted probability, and Ω regularizes the complexity of K trees. This regularization prevents overfitting while maintaining high predictive accuracy on GPS signal features.

Second, Random Forest is integrated to reduce variance via bagging and random feature subspace selection. Multiple decision trees are constructed independently using bootstrap samples, and the final prediction is obtained through majority voting. The random subspace method ensures that each tree considers only a subset of features at each split, thereby decorrelating the individual trees and enhancing ensemble robustness. These tree-based models capture non-linear relationships within the GPS signal metrics effectively.

Third, TabNet is incorporated as a deep learning component specifically designed for tabular data. Unlike standard neural networks that process all features simultaneously, TabNet employs a sequential attention transformer mechanism to select relevant features at each decision step, enabling instance-wise feature selection and improved interpretability. The architecture consists of multiple decision steps, where each step processes a subset of salient features.

The input feature vector $\mathbf{x} \in \mathbb{R}^{13}$ is first normalized through batch normalization:

$$\mathbf{BN}(\mathbf{x}) = \gamma \frac{\mathbf{x} - \mu}{\sqrt{\sigma^2 + \epsilon}} + \beta \tag{2}$$

where μ and σ^2 denote the batch mean and variance, while γ and β are learnable parameters. At each decision step t, an attention mask $\mathbf{M}_t \in \mathbb{R}^{13}$ is computed through a sparsemax transformation to identify the subset of features contributing to the decision:

$$\mathbf{M}_t = \text{sparsemax}(\mathbf{W}_a \mathbf{h}_{t-1} + \mathbf{b}_a) \tag{3}$$

where $\mathbf{h}_{t-1}$ represents the hidden state from the previous step, $\mathbf{W}_a$ denotes the attention weight matrix, and $\mathbf{b}_a$ is the bias term. The sparsemax function produces a sparse probability distribution, effectively zeroing out irrelevant features.

The selected features are then transformed through a feature transformer block consisting of gated linear units:

$$\mathbf{f}_t = \text{GLU}(\mathbf{W}_f[\mathbf{x} \odot \mathbf{M}_t]) = \sigma(\mathbf{W}_1[\mathbf{x} \odot \mathbf{M}_t]) \odot (\mathbf{W}_2[\mathbf{x} \odot \mathbf{M}_t]) \tag{4}$$

where $\odot$ denotes element-wise multiplication, σ is the sigmoid activation, and $\mathbf{W}_f$ represents the transformation weights. The hidden state is updated recursively:

$$\mathbf{h}_t = \text{ReLU}(\mathbf{W}_h \mathbf{h}_{t-1} + \mathbf{f}_t) \tag{5}$$

The outputs from all decision steps are aggregated to produce the final representation:

$$\mathbf{d}_{\text{out}} = \sum_{t=1}^{N_{\text{steps}}} \text{ReLU}(\mathbf{d}_t) \tag{6}$$

 doi:10.20944/preprints202604.1124.v1

where $\mathbf{d}_t$ denotes the decision output at step t. This multi-step processing allows the model to focus on discriminative signal characteristics, such as PD or CN0, while suppressing noise and redundant information.

The hyperparameters of TabNet are configured as follows: the decision embedding dimension n_d and attention embedding dimension n_a are both set to 128, the number of decision steps N_{steps} is set to 3, and the sparsity coefficient γ is set to 1.3 to control the trade-off between feature selection sparsity and information retention. The model is optimized using the Adam optimizer with a learning rate of 3×10^{-3} and a step learning rate scheduler.

The output probabilities from TabNet complement the tree-based models by capturing complex high-order interactions that may be overlooked by gradient boosting or bagging approaches. By integrating these three heterogeneous base learners within the stacking framework, the proposed Stack-TabNet model leverages their complementary strengths: the gradient-based optimization of XGBoost, the variance reduction of Random Forest, and the attention-driven feature selection of TabNet. This diversity is expected to enhance generalization capability across diverse spoofing attack scenarios, and the experimental results demonstrate that the ensemble indeed surpasses the performance of each individual base classifier.

2.2.2. Stacking Mechanism and Meta-Learning

The predictions from the base learners are combined using a stacking generalization strategy. Instead of hard class labels, the predicted class probabilities are utilized as input features for the second level. This approach preserves uncertainty information and provides a richer representation for the meta-learner. Specifically, the probability vector $\mathbf{p}_i = [p_{i,0}, p_{i,1}, p_{i,2}, p_{i,3}]$ generated by each base classifier i is concatenated.

Additionally, the original input features are retained and passed to the meta-learner to prevent information loss. Consequently, the meta-learner receives a concatenated vector comprising both the base predictions and the original input features. The meta-learner is implemented using Logistic Regression with a multinomial loss function. This linear model is chosen to minimize the risk of overfitting given the reduced dimensionality of the meta-features. The final prediction $\hat{y}$ is derived by maximizing the probability output from the meta-learner:

$$\hat{y} = \arg\max_c(\text{softmax}(\mathbf{W}_{meta}[\mathbf{p}_{XGB}, \mathbf{p}_{RF}, \mathbf{p}_{TabNet}, \mathbf{x}] + \mathbf{b}_{meta})) \tag{7}$$

where $\mathbf{W}_{meta}$ and $\mathbf{b}_{meta}$ represent the weights and bias of the logistic regression model, $\mathbf{x}$ denotes the original input feature vector, and $\mathbf{p}_{XGB}$, $\mathbf{p}_{RF}$, and $\mathbf{p}_{TabNet}$ denote the class probability vectors generated by the XGBoost, Random Forest, and TabNet base learners, respectively.

2.2.3. Training Strategy

The ensemble model is trained on the balanced dataset obtained through random under-sampling. This preprocessing step mitigates the bias towards the majority class observed in the raw data. During training, the base learners are fitted independently. Subsequently, out-of-fold predictions are generated to train the meta-learner, ensuring that the stacking process remains robust against data leakage. The optimization objective focuses on maximizing classification accuracy while maintaining computational efficiency suitable for potential real-time deployment. By integrating TabNet's interpretable attention masks with the stability of tree ensembles, the Stack-TabNet framework achieves a balance between performance and transparency.

2.3. Feature Interpretability and Selection Policy

While the proposed Stack-TabNet framework delivers robust detection performance, the opacity of deep learning components necessitates a rigorous interpretability analysis to ensure trustworthiness in safety-critical navigation applications. To address this, SHAP is employed to quantify the contribution of each input feature to the model's output. SHAP is grounded in cooperative game theory, where the

 doi:10.20944/preprints202604.1124.v1

Shapley value provides a unique solution for fairly distributing the "payout" (prediction) among the "players" (features). For a given prediction, the SHAP value ϕ_i for feature i is formulated as:

$$\phi_i = \sum_{S \subseteq N \setminus \{i\}} \frac{|S|!(|N| - |S| - 1)!}{|N|!} [f(S \cup \{i\}) - f(S)] \tag{8}$$

where N denotes the set of all features, S represents a subset of features excluding i, and f is the model prediction function. This formulation ensures properties of local accuracy, missingness, and consistency, making it superior to traditional perturbation-based methods.

Given the hybrid nature of the ensemble, SHAP analysis is primarily conducted on the TabNet base learner using the DeepExplainer algorithm, which is optimized for deep neural networks. A background dataset is sampled from the training set to estimate the expected model output. For each sample in the evaluation set, SHAP values are computed across all 13 input features and four target classes. To derive a global measure of feature importance, the mean absolute SHAP value is calculated for each feature across the entire dataset:

$$I_i = \frac{1}{M} \sum_{j=1}^{M} |\phi_i^{(j)}| \tag{9}$$

where I_i represents the importance score of feature i, M is the number of samples, and $\phi_i^{(j)}$ is the SHAP value for feature i on sample j. Features are subsequently ranked in descending order based on I_i.

Based on the ranking results, a feature selection policy is implemented to construct an optimized variant of the proposed model. Specifically, a subset of features exhibiting the highest discriminative power is retained, while the remaining features with lower contribution scores are excluded. This subset is expected to comprise critical signal metrics that consistently demonstrate strong attribution values across different spoofing classes. The rationale behind this strategy is twofold. First, removing features with negligible SHAP values mitigates the influence of noise and redundant information, which can otherwise degrade generalization capability. Second, reducing the input dimensionality lowers the computational overhead during both training and inference, enhancing suitability for real-time deployment.

This optimized configuration is designated as Stack-TabNet-2, whereas the model utilizing all available features is referred to as Stack-TabNet-1. It is hypothesized that the curated feature subset enables the ensemble to focus on the most salient signal characteristics, thereby improving classification accuracy. The comparative performance of these two variants is empirically validated in the **experimental section** to evaluate the effectiveness of SHAP-driven feature selection in improving model's performance without compromising detection integrity.

3. Experiments and Results

3.1. Experimental Setup

All experiments are conducted on a high-performance workstation equipped with an Intel Core i9-1400K processor operating at 3200 MHz, 128 GB of Kingston DDR5 memory and an NVIDIA RTX 5090 graphics processing unit. The implementation is based on Python with scikit-learn and PyTorch libraries.

To address the inherent class imbalance in the raw GPS spoofing dataset, Random Undersampling is applied to achieve balanced class distributions across all four categories. The classes are encoded as integers: Class 0 represents Authentic signals, Class 1 denotes Simplistic attacks, Class 2 indicates Intermediate attacks, and Class 3 corresponds to Sophisticated attacks. The dataset is partitioned into training and testing subsets with a 75:25 ratio. The detailed data distribution is presented in Table 2.

 doi:10.20944/preprints202604.1124.v1

Table 2. Dataset Distribution After Random Undersampling.

Category	Number of Samples
Total number of samples	128,060
Training samples (75.00%)	96,045
Testing samples (25.00%)	32,015
Class Distribution in Training Set	
Class 0 (Authentic)	23,964
Class 1 (Simplistic)	23,886
Class 2 (Intermediate)	24,042
Class 3 (Sophisticated)	24,153
Class Distribution in Testing Set	
Class 0 (Authentic)	8,051
Class 1 (Simplistic)	8,129
Class 2 (Intermediate)	7,973
Class 3 (Sophisticated)	7,862

3.2. Comparative Experiments

To comprehensively evaluate the effectiveness of the proposed Stack-TabNet ensemble framework, comparative experiments are conducted against eight baseline models, including Decision Tree [23], Gaussian Naive Bayes [24], K-Nearest Neighbor [25], Logistic Regression [26] Random Forest [27], Support Vector Machines [28], XGBoost [29], and standalone TabNet [30]. All models are trained on the same balanced training set and evaluated on the identical testing set to ensure fair comparison.

3.2.1. Confusion Matrix Analysis

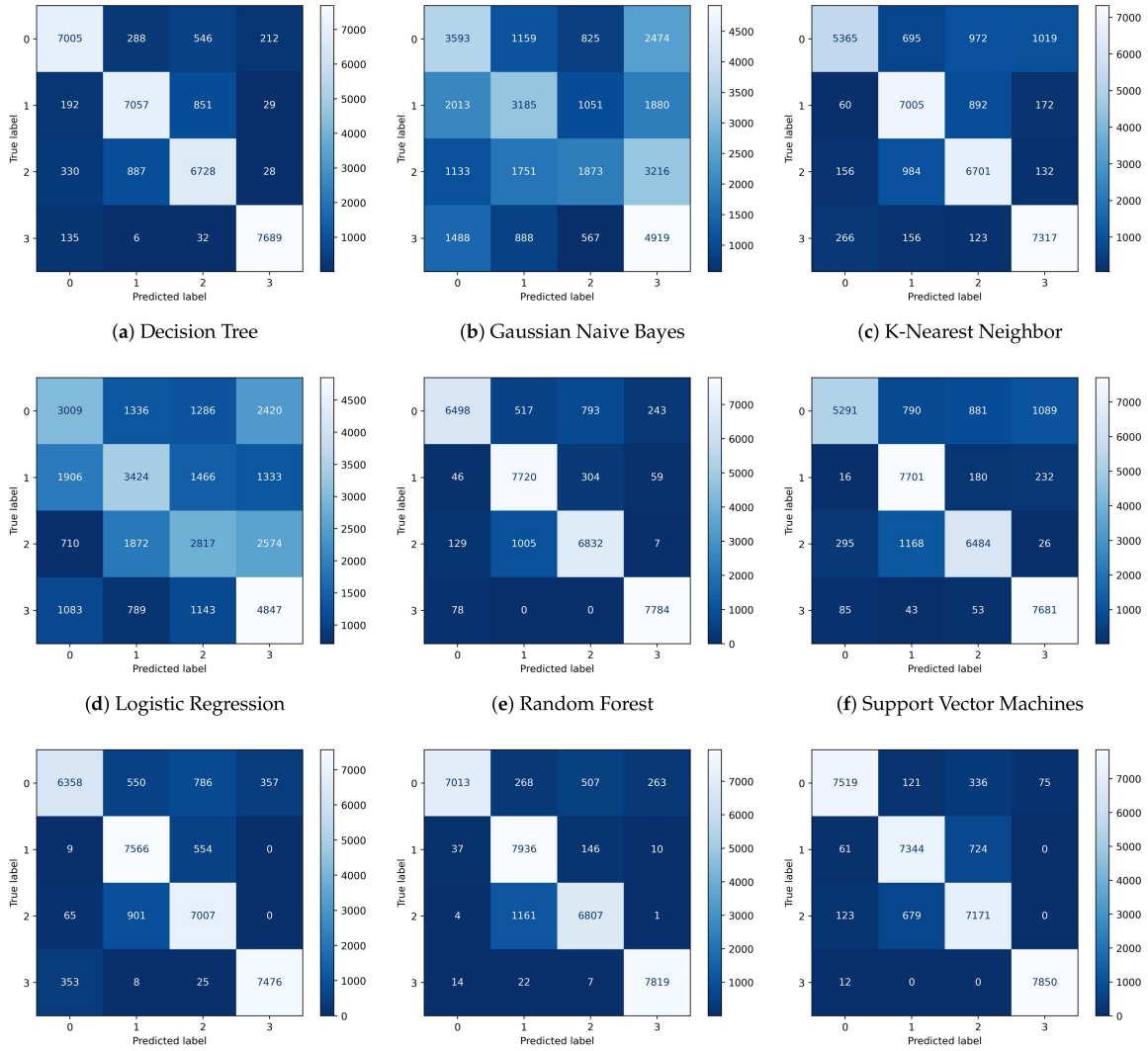
The confusion matrices for all nine models are presented in Figure 5. Each matrix illustrates the classification performance across the four spoofing categories, where the diagonal elements represent correctly classified samples and off-diagonal elements indicate misclassifications.

From the visualized results, it is observed that traditional machine learning models such as Gaussian Naive Bayes and Logistic Regression exhibit substantial confusion between authentic and spoofed signals, particularly for Class 1 and Class 2 attacks. In contrast, ensemble methods including Random Forest, XGBoost, and the proposed Stack-TabNet1 demonstrate superior discrimination capability with minimal off-diagonal errors. The Stack-TabNet1 model achieves the highest diagonal concentration, indicating robust classification across all attack types.

3.2.2. ROC-AUC Curve Analysis

The Receiver Operating Characteristic (ROC) curves and Area Under the Curve (AUC) values for all models are illustrated in Figure 6. The ROC curves are plotted for each of the four classes using a one-vs-rest approach, providing a comprehensive view of model performance across different decision thresholds.

 doi:10.20944/preprints202604.1124.v1



(**a**) Decision Tree (**b**) Gaussian Naive Bayes (**c**) K-Nearest Neighbor

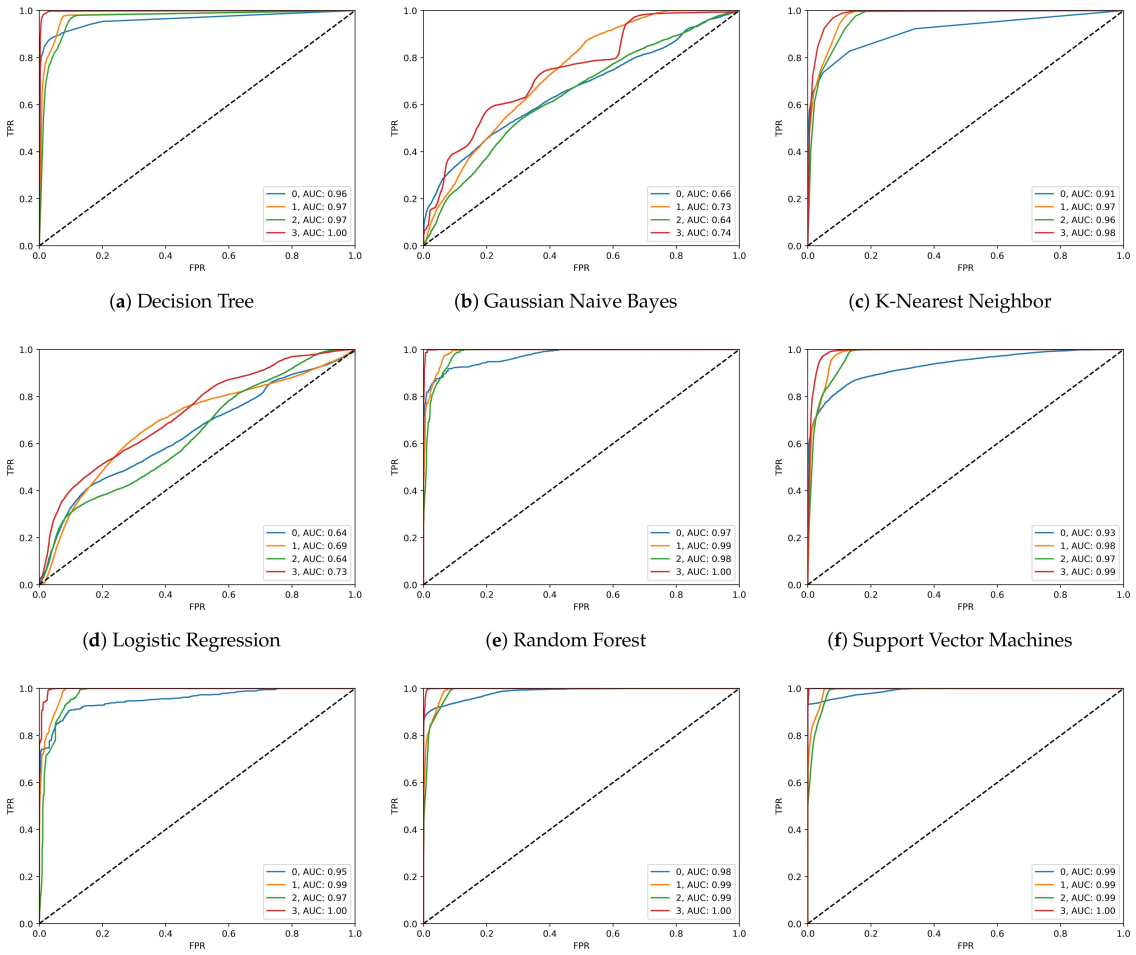
(**d**) Logistic Regression (**e**) Random Forest (**f**) Support Vector Machines

(**g**) XGBoost (**h**) TabNet (**i**) Stack-TabNet1

Figure 5. This is a figure. Schemes follow the same formatting.

The Stack-TabNet1 model demonstrates consistently high AUC values across all classes, with particularly strong performance in distinguishing sophisticated attacks (Class 3). The ensemble architecture effectively combines the strengths of tree-based models and attention-driven deep learning, resulting in improved separability between authentic and spoofed signal patterns.

 doi:10.20944/preprints202604.1124.v1



(**a**) Decision Tree (**b**) Gaussian Naive Bayes (**c**) K-Nearest Neighbor

(**d**) Logistic Regression (**e**) Random Forest (**f**) Support Vector Machines

(**g**) XGBoost (**h**) TabNet (**i**) Stack-TabNet1

Figure 6. This is a figure. Schemes follow the same formatting.

3.2.3. Per-Class Performance Metrics

The precision, recall, and F1-score for each model across all four classes are summarized in Tables 3, 4, and 5, respectively. These metrics provide granular insights into model behavior for each spoofing category.

Table 3. Precision Comparison Across Nine Models for Four GPS Spoofing Classes.

Model	Class 0	Class 1	Class 2	Class 3	Macro Avg
Decision Tree	0.9152	0.8563	0.8251	0.9675	0.8910
Gaussian Naive Bayes	0.4369	0.4589	0.4375	0.3943	0.4319
K-Nearest Neighbor	0.9085	0.7896	0.7677	0.8439	0.8274
Logistic Regression	0.4487	0.4629	0.4195	0.4338	0.4412
Random Forest	0.9675	0.8328	0.8659	0.9634	0.9074
Support Vector Machines	0.9265	0.7863	0.6914	0.8492	0.8134
XGBoost	0.9368	0.8372	0.8354	0.9500	0.8899
TabNet	0.9847	0.8462	0.9150	0.9612	0.9268
Stack-TabNet1	**0.9765**	**0.9038**	**0.9349**	**0.9905**	**0.9514**

 doi:10.20944/preprints202604.1124.v1

Table 4. Recall Comparison Across Nine Models for Four GPS Spoofing Classes.

Model	Class 0	Class 1	Class 2	Class 3	Macro Avg
Decision Tree	0.8693	0.8636	0.8438	0.9778	0.8886
Gaussian Naive Bayes	0.4476	0.3898	0.4025	0.6246	0.4661
K-Nearest Neighbor	0.6684	0.8574	0.8395	0.9326	0.8245
Logistic Regression	0.3749	0.4190	0.3531	0.6154	0.4406
Random Forest	0.8064	0.9448	0.8560	0.9883	0.8989
Support Vector Machines	0.6592	0.9408	0.8123	0.9752	0.8469
XGBoost	0.7921	0.9261	0.8779	0.9492	0.8863
TabNet	0.8737	0.9754	0.8530	0.9928	0.9237
Stack-TabNet1	**0.9369**	**0.9008**	**0.8985**	**0.9987**	**0.9337**

Table 5. F1-Score Comparison Across Nine Models for Four GPS Spoofing Classes.

Model	Class 0	Class 1	Class 2	Class 3	Macro Avg
Decision Tree	0.8916	0.8600	0.8344	0.9726	0.8897
Gaussian Naive Bayes	0.4422	0.4215	0.4196	0.4833	0.4416
K-Nearest Neighbor	0.7707	0.8220	0.8020	0.8861	0.8202
Logistic Regression	0.4085	0.4400	0.3849	0.5090	0.4356
Random Forest	0.8796	0.8852	0.8609	0.9757	0.9004
Support Vector Machines	0.7704	0.8567	0.7468	0.9079	0.8205
XGBoost	0.8584	0.8794	0.8561	0.9496	0.8859
TabNet	0.9259	0.9060	0.8830	0.9767	0.9229
Stack-TabNet1	**0.9563**	**0.9023**	**0.9163**	**0.9946**	**0.9424**

From the per-class metrics, several observations are made. First, Gaussian Naive Bayes and Logistic Regression perform poorly across all classes, with F1-scores below 0.50, indicating their inadequacy for complex GPS spoofing detection tasks. Second, tree-based ensemble methods including Random Forest and XGBoost demonstrate competitive performance, particularly for Class 3 sophisticated attacks. Third, TabNet achieves strong results through its attention mechanism, but the proposed Stack-TabNet1 further improves performance by integrating complementary model strengths. Notably, Stack-TabNet1 achieves the highest precision score 0.9905 for Class 3 and the highest recall score 0.9987 for Class 3, demonstrating exceptional capability in identifying sophisticated spoofing attempts.

3.2.4. Overall Accuracy Comparison

The overall classification accuracy for all nine models is summarized in Table 6. This metric provides a holistic view of model performance across all spoofing categories.

Results demonstrate that the proposed Stack-TabNet1 achieves the highest overall accuracy of 93.37%, outperforming the second-best model TabNet by 1.00 percentage points. Compared to traditional machine learning baselines, the improvement is more substantial, with gains of 3.48% over Random Forest and 4.74% over XGBoost. The inferior performance of Gaussian Naive Bayes and Logistic Regression below 50% accuracy highlights the complexity of GPS spoofing detection and the necessity of advanced ensemble or deep learning approaches. The consistent superiority of Stack-TabNet1 across all evaluation metrics validates the effectiveness of integrating TabNet attention-driven feature selection with the stability of tree-based ensemble methods within a stacking framework.

 doi:10.20944/preprints202604.1124.v1

Table 6. Overall Performance Comparison Across Nine Models.

Model	Weighted Precision	Weighted Recall	Weighted F1-Score	Accuracy (%)
Gaussian Naive Bayes	0.4320	0.4661	0.4417	46.61
Logistic Regression	0.4413	0.4406	0.4357	44.06
K-Nearest Neighbor	0.8275	0.8245	0.8203	82.45
Support Vector Machines	0.8135	0.8469	0.8206	84.69
XGBoost	0.8899	0.8863	0.8860	88.63
Decision Tree	0.8896	0.8896	0.8896	88.96
Random Forest	0.9075	0.8989	0.9005	89.89
TabNet	0.9268	0.9237	0.9230	92.37
Stack-TabNet1	**0.9515**	**0.9337**	**0.9425**	**93.37**

3.3. SHAP Interpretability Analysis

To enhance the transparency and trustworthiness of the proposed Stack-TabNet1 model, SHAP is employed to interpret the feature contributions across all four GPS spoofing categories. SHAP provides a unified measure of feature importance based on cooperative game theory, ensuring properties of local accuracy, consistency, and missingness. The analysis is conducted on 2,000 test samples using a DeepExplainer optimized for deep neural network architectures. Three types of visualizations are generated: SHAP violin plots illustrating the distribution of feature impacts, SHAP bar plots ranking features by their mean absolute SHAP values, and SHAP dependence plots revealing the relationship between feature values and their corresponding SHAP values.

3.3.1. SHAP Violin Plot Analysis

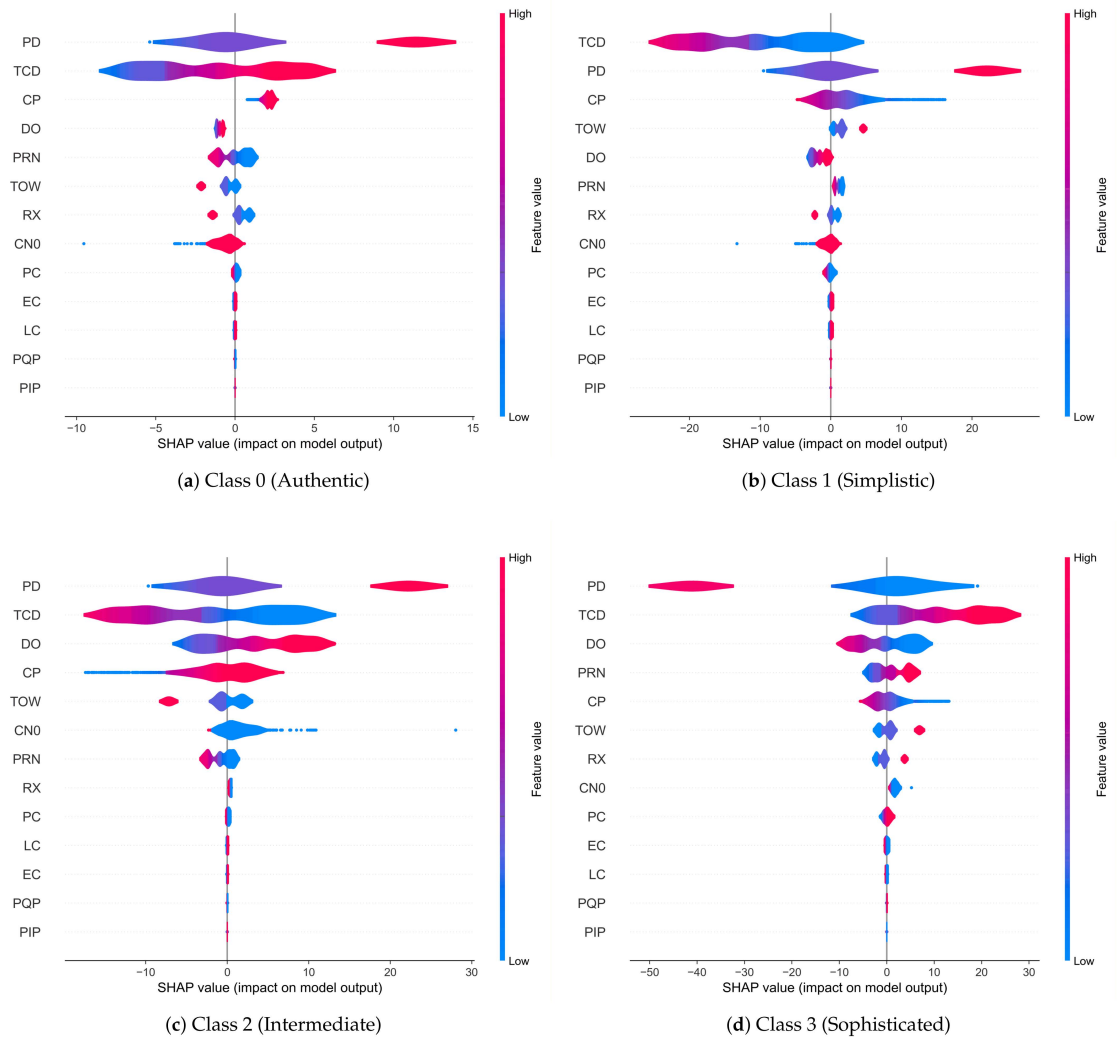
The SHAP violin plots for all four classes are presented in Figure 7. Each violin plot displays the distribution of SHAP values for the 13 input features, where the width of the violin represents the density of samples at each SHAP value level. Positive SHAP values indicate features that push the model prediction toward the corresponding class, while negative values indicate features that push the prediction away from that class.

From Figure 7, several observations are made. First, PD and TCD consistently exhibit the widest distributions across all classes, indicating their dominant role in distinguishing between authentic and spoofed signals. Second, the SHAP value distributions for correlation-based features including EC, LC and PC are relatively narrow, suggesting their limited contribution to the final decision. Third, Class 3 demonstrates the most pronounced SHAP value separation, which aligns with the model's high recall score 0.9987 for this category. The violin plots confirm that the Stack-TabNet1 model relies on physically meaningful signal characteristics rather than spurious correlations.

3.3.2. Feature Importance Ranking

The global feature importance rankings for all four classes are illustrated in Figure 8. The mean absolute SHAP value is computed for each feature across all test samples, providing a quantitative measure of each feature's overall contribution to the model output.

 doi:10.20944/preprints202604.1124.v1



(**a**) Class 0 (Authentic)

(**b**) Class 1 (Simplistic)

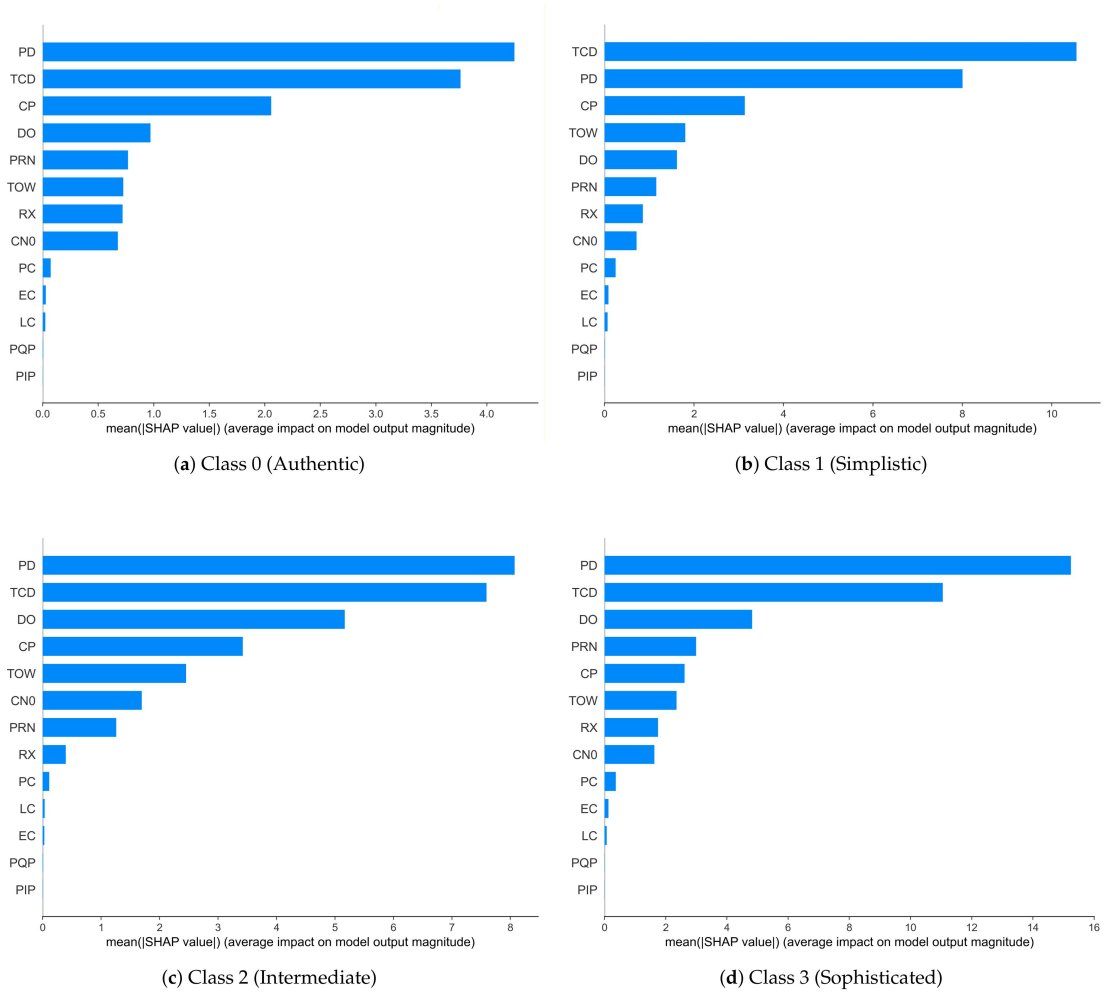
(**c**) Class 2 (Intermediate)

(**d**) Class 3 (Sophisticated)

Figure 7. This is a figure. Schemes follow the same formatting.

As shown in Figure 8, PD and TCD emerge as the two most important features across all four classes, with mean absolute SHAP values ranging from 4.25 to 15.25 depending on the class. For Class 0, the top five features are PD at 4.25, TCD at 3.76, CP at 2.06, DO at 0.97, and PRN at 0.77. For Class 3, the ranking shifts slightly with PD at 15.25, TCD at 11.06, DO at 4.83, PRN at 3.00, and CP at 2.62. This consistency validates the physical interpretability of the model, as pseudorange and code delay are fundamental indicators of signal authenticity in GPS receivers. Notably, while TCD and DO exhibit strong linear correlation, their simultaneous retention is justified by their distinct physical definitions in signal tracking loops and the non-linear capacity of the ensemble model to utilize them complementarily rather than redundantly. Besides, the importance of PD increases substantially for Class 3, reflecting the model ability to detect subtle anomalies in distance measurements that characterize advanced spoofing techniques.

 doi:10.20944/preprints202604.1124.v1



(**a**) Class 0 (Authentic)

(**b**) Class 1 (Simplistic)

(**c**) Class 2 (Intermediate)

(**d**) Class 3 (Sophisticated)

Figure 8. This is a figure. Schemes follow the same formatting.

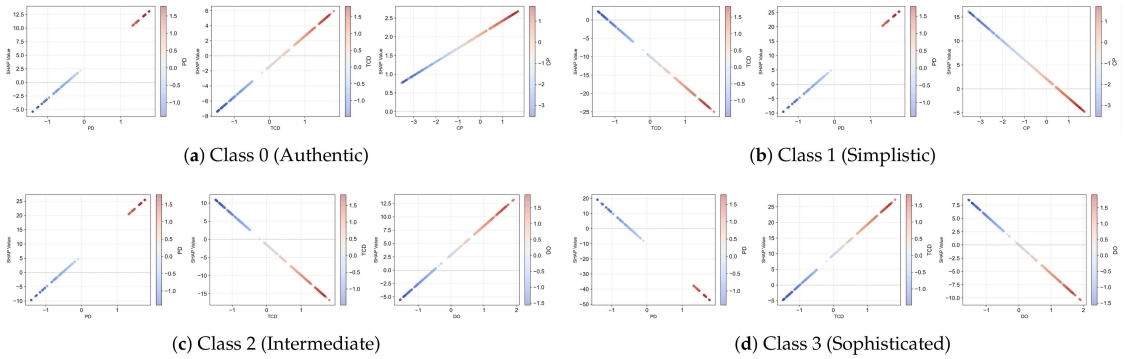
3.3.3. SHAP Dependence Plot Analysis

The SHAP dependence plots for the top three features of each class are displayed in Figure 9. Each scatter plot shows the relationship between a feature value on the horizontal axis and its corresponding SHAP value on the vertical axis, revealing how changes in feature values influence the model prediction.

Clear monotonic relationships are observed between PD, TCD and their SHAP values across all classes from Figure 9. For Class 3, PD exhibits a strong positive correlation with SHAP values, where higher pseudorange measurements correspond to increased likelihood of sophisticated spoofing detection. This aligns with the physical principle that spoofed signals often introduce anomalous distance estimates. Similarly, TCD demonstrates consistent negative correlations, where abnormal code delay patterns indicate potential spoofing interference. The dependence plots confirm that the Stack-TabNet1 model captures physically interpretable relationships between GPS signal characteristics and spoofing attack patterns, rather than relying on opaque feature combinations.

SHAP analysis reveals that while all 13 features contribute to the model decision-making process, their importance varies significantly across different spoofing categories. PD and TCD consistently dominate the feature importance rankings, while correlation-based features such as EC, LC, and PC and quadrature components such as PIP and PQP exhibit relatively minor contributions. This suggests that a subset of highly discriminative features may be sufficient to achieve comparable or even superior detection performance, as removing low-importance features can reduce noise and computational overhead without compromising accuracy. The implications of this finding are explored in the subsequent section through the development of an optimized model variant utilizing SHAP-driven feature selection.

 doi:10.20944/preprints202604.1124.v1



(**a**) Class 0 (Authentic) (**b**) Class 1 (Simplistic)

(**c**) Class 2 (Intermediate) (**d**) Class 3 (Sophisticated)

Figure 9. This is a figure. Schemes follow the same formatting.

3.4. SHAP-Driven Feature Selection and Stack-TabNet2 Performance

Based on the SHAP interpretability analysis conducted in the previous section, an optimized model variant designated as Stack-TabNet2 is developed. The top 8 features including PD, TCD, DO, CP, PRN, TOW, RX, and CN0, exhibiting the highest mean absolute SHAP values across all four spoofing categories are selected for training, while the remaining 5 features with lower contribution scores are excluded. Although SHAP values are primarily derived from the TabNet component to leverage its intrinsic attention mechanism, the resulting feature subset is empirically validated on the full stacking ensemble to ensure compatibility and performance across all base learners. The Stack-TabNet2 architecture maintains identical configuration to Stack-TabNet1.

3.4.1. Performance Evaluation of Stack-TabNet2

The classification performance of Stack-TabNet2 is comprehensively evaluated using the same testing set as Stack-TabNet1 to ensure fair comparison. The per-class precision, recall, and F1-score metrics are summarized in Table 7.

Table 7. Per-Class Performance Metrics of Stack-TabNet2 Model.

Metric	Class 0	Class 1	Class 2	Class 3	Macro Avg
Precision	0.9786	0.9539	0.9584	0.9926	0.9709
Recall	0.9545	0.9448	0.9393	0.9978	0.9591
F1-Score	0.9664	0.9493	0.9488	0.9952	0.9649

The confusion matrix for Stack-TabNet2 is presented in Figure 10. The diagonal elements indicate correctly classified samples, while off-diagonal elements represent misclassifications. Compared to Stack-TabNet1, Stack-TabNet2 demonstrates improved classification accuracy with reduced confusion between Simplistic and Intermediate attacks.

The ROC-AUC curves for Stack-TabNet2 across all four classes are illustrated in Figure 11. The model achieves near-perfect AUC values of 1.00 for Class 0 (Authentic), Class 1 (Simplistic), and Class 3 (Sophisticated), with 0.99 for Class 2 (Intermediate). These results indicate exceptional discrimination capability despite the reduced feature dimensionality.

 doi:10.20944/preprints202604.1124.v1

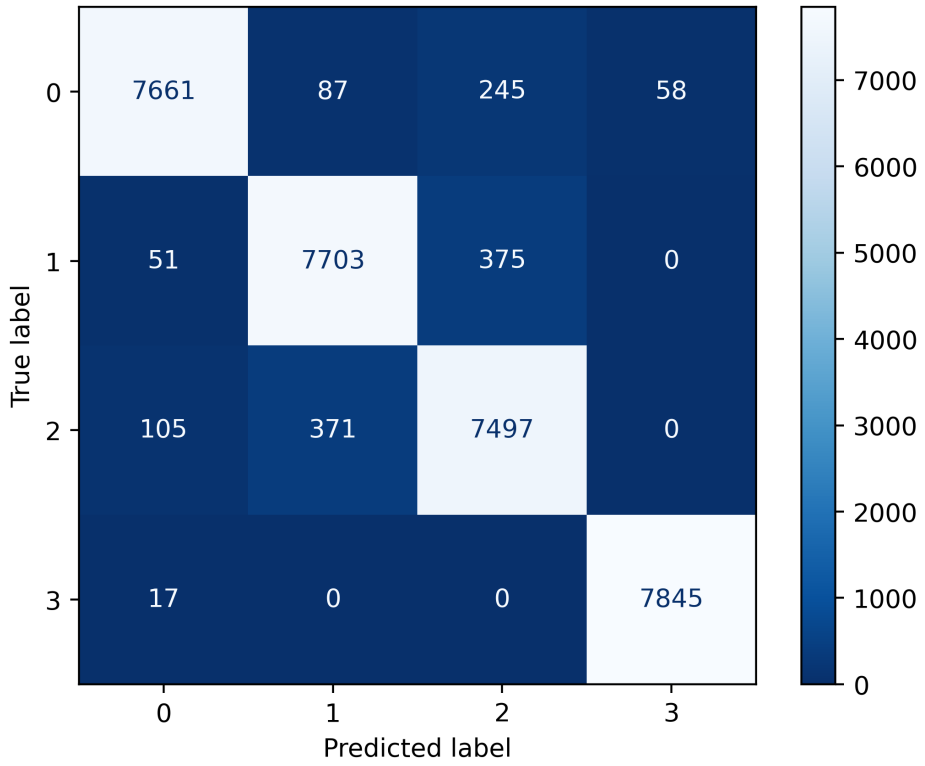


Figure 10. Confusion matrix of Stack-TabNet2 model. The diagonal elements represent correctly classified samples (Class 0: 7661, Class 1: 7703, Class 2: 7497, Class 3: 7845), while off-diagonal elements indicate misclassifications. Stack-TabNet2 achieves 95.91% overall accuracy with only 8 input features.

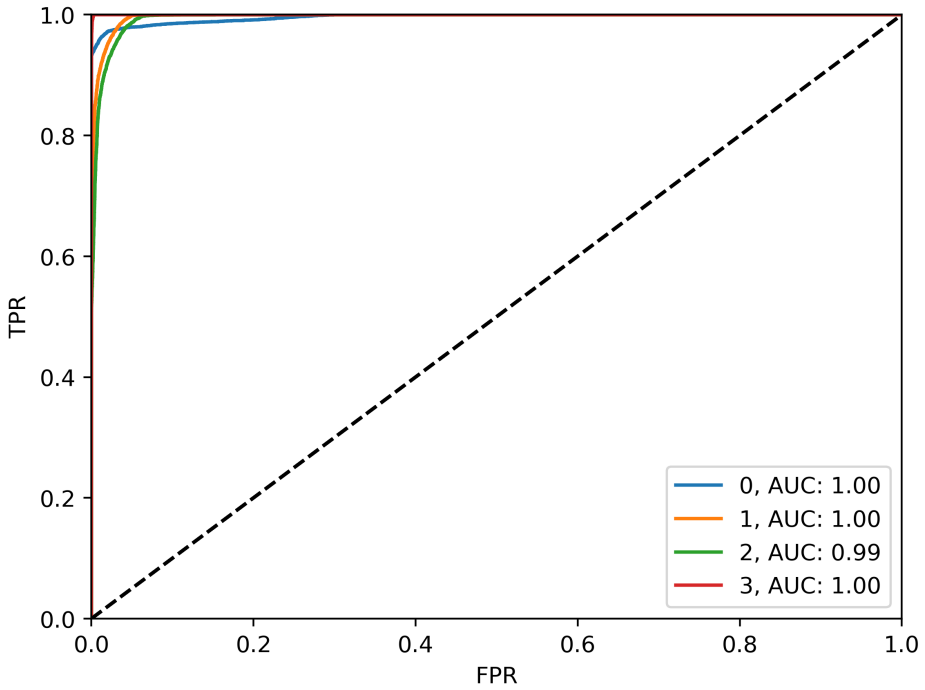


Figure 11. ROC-AUC curves of Stack-TabNet2 model for four GPS spoofing classes. The model achieves AUC values of 1.00 for Class 0, Class 1, and Class 3, and 0.99 for Class 2, demonstrating superior separability between authentic and spoofed signal patterns with only 8 input features.

 doi:10.20944/preprints202604.1124.v1

3.4.2. Comparative Analysis: Stack-TabNet1 vs. Stack-TabNet2

A comprehensive comparison between Stack-TabNet1 (13 features) and Stack-TabNet2 (8 features) is presented in Table 8. Remarkably, Stack-TabNet2 achieves higher overall accuracy (95.91%) compared to Stack-TabNet1 (93.37%), despite utilizing 38.5% fewer input features.

Table 8. Performance Comparison Between Stack-TabNet1 and Stack-TabNet2.

Model	Input Features	Weighted F1-Score	Accuracy (%)
Stack-TabNet1	13	0.9425	93.37
Stack-TabNet2	8	0.9649	95.91
Improvement	**-5 features (-38.5%)**	**+2.37%**	**+2.54%**

Several observations are made from this comparison. First, the removal of 5 low-importance features (EC, LC, PC, PIP, PQP) eliminates redundant information and reduces noise interference, leading to improved generalization capability. Second, the computational overhead during both training and inference is significantly reduced, enhancing suitability for real-time deployment on resource-constrained platforms. Third, the consistency of PD and TCD as the top two features across all classes validates their fundamental role in GPS spoofing detection, as these metrics directly reflect signal propagation anomalies introduced by adversarial transmitters.

The superior performance of Stack-TabNet2 demonstrates that SHAP-driven feature selection effectively identifies the most discriminative signal characteristics while discarding features with negligible contribution. This finding has important implications for practical GPS anti-spoofing system design, where computational efficiency and detection accuracy must be balanced under real-world operational constraints.

4. Discussion

The experimental results validate the effectiveness of the proposed Stack-TabNet framework for GPS spoofing detection across diverse attack scenarios. The comparative analysis demonstrates that the ensemble approach consistently outperforms individual baseline models, including standalone TabNet, XGBoost, and Random Forest. Specifically, the optimized Stack-TabNet2 variant achieves an accuracy of 95.91%, surpassing the 93.37% accuracy of the full-feature Stack-TabNet1 model. This improvement underscores the efficacy of the SHAP-driven feature selection strategy, which mitigates the influence of redundant features and reduces noise within the input data. The integration of TabNet's attention mechanism with tree-based models leverages complementary strengths, resulting in enhanced robustness against simplistic, intermediate, and sophisticated spoofing attacks. The high recall rates observed for Class 3 (Sophisticated Attacks) indicate that the model successfully captures subtle signal anomalies that traditional methods often overlook.

The interpretability analysis provided by SHAP offers critical insights into the decision-making process of the deep learning model, addressing the "black-box" concern prevalent in safety-critical aviation applications. The feature importance rankings reveal that PD and TCD consistently contribute the most to classification decisions across all classes. This aligns with the physical principles of GPS spoofing, where adversarial signals typically introduce inconsistencies in signal propagation time and distance measurements. By visualizing these contributions, the study establishes trust in the model's predictions, allowing system operators to understand why a specific signal is flagged as spoofed. Furthermore, the dependence plots illustrate non-linear relationships between feature values and model output, confirming that the model learns complex patterns rather than relying on simple thresholding. This transparency is essential for regulatory approval and practical deployment in autonomous navigation systems.

Despite the promising results, certain limitations warrant consideration. The computational complexity of the stacking ensemble, although reduced in Stack-TabNet2, remains higher than that of single

 doi:10.20944/preprints202604.1124.v1

lightweight models, which may pose challenges for real-time deployment on resource-constrained UAVs. Additionally, the model is trained and evaluated on a specific dataset; its generalizability to other GNSS constellations (e.g., Galileo, GLONASS) or different environmental conditions requires further validation. The current study focuses on supervised learning, which relies on labeled data that may be scarce in real-world spoofing incidents. Future work addresses these limitations by exploring model compression techniques, such as knowledge distillation, to facilitate edge deployment. Further research also extends the framework to multi-constellation GNSS environments and investigates semi-supervised learning approaches to reduce reliance on labeled spoofing data. Finally, the integration of this detection module into a resilient navigation framework that can switch to alternative positioning sources upon detection constitutes a vital direction for subsequent research.

5. Conclusions

In this study, an interpretable ensemble learning framework designated as Stack-TabNet is proposed for GPS spoofing detection with systematic feature selection to address the limitations of existing methods in generalization and transparency. The architecture integrates the attention-based TabNet network with XGBoost and Random Forest within a stacking mechanism, while SHAP analysis provides comprehensive interpretability by quantifying feature contributions across all spoofing categories. Experimental results demonstrate that the optimized variant, Stack-TabNet2, achieves an accuracy of 95.91%, surpassing both standalone baseline models and the full-feature Stack-TabNet1 variant. The SHAP-driven feature selection identifies Pseudorange and Time of Code Delay as the most discriminative features, enabling effective dimensionality reduction from 13 to 8 inputs without compromising detection integrity. This confirms that interpretable feature selection not only reduces computational overhead but also enhances model transparency by revealing physically meaningful signal characteristics underlying spoofing detection. Consequently, the proposed method provides a transparent and efficient solution for safeguarding navigation systems against diverse spoofing attacks, offering significant potential for real-time deployment in safety-critical applications where both accuracy and interpretability are paramount.

Author Contributions: Conceptualization, T.C.; Methodology, T.C.; Software, T.C.; Validation, T.C.; formal analysis, T.C.; writing—original draft preparation, T.C.; writing—review and editing, Q.S., G.P., L.S., H.Z., J.Z. and T.C.; Visualization, T.C.; project administration, G.P. All authors have read and agreed to the published version of the manuscript.

Data Availability Statement: The GPS Spoofing dataset presented in this paper are available on request from [22].

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Wang, S.; Ahmad, N.S. A Comprehensive Review on Sensor Fusion Techniques for Localization of a Dynamic Target in GPS-Denied Environments. *IEEE Access* **2025**, *13*, 2252–2285. https://doi.org/10.1109/ACCESS.2024.3519874.
2. Chen, X.; Ge, M.; Männel, B.; Schuh, H. Analysis of periodic terms in the DYB frame for the solar radiation pressure model of BDS-3 MEO satellites. *GPS Solutions* **2025**, *29*, 90.
3. Chen, X.; Ge, M.; Männel, B.; Hugentobler, U.; Schuh, H. Extending higher-order model for non-conservative perturbing forces acting on Galileo satellites during eclipse periods. *98*, 113. https://doi.org/10.1007/s00190-024-01924-4.
4. Meng, L.; Yang, L.; Yang, W.; Zhang, L. A Survey of GNSS Spoofing and Anti-Spoofing Technology. *Remote Sensing* **2022**, *14*. https://doi.org/10.3390/rs14194826.
5. Lu, C.; Lu, Z.; Liu, Z.; Huang, L.; Chen, F. Overview of satellite nav spoofing and anti-spoofing techniques. *12*. https://doi.org/10.3389/fphy.2024.1428544.
6. Zhang, B.; Yang, C.; Xiao, G.; Li, P.; Xiao, Z.; Wei, H.; Liu, J. Loosely Coupled PPP/Inertial/LiDAR Simultaneous Localization and Mapping (SLAM) Based on Graph Optimization. *Remote Sensing* **2025**, *17*. https://doi.org/10.3390/rs17050812.

 doi:10.20944/preprints202604.1124.v1

7. Xiao, G.; Yang, C.; Wei, H.; Xiao, Z.; Zhou, P.; Li, P.; Dai, Q.; Zhang, B.; Yu, C. PPP ambiguity resolution based on factor graph optimization. *GPS solutions* **2024**, *28*, 178.
8. Zhou, P.; Nie, Z.; Xiang, Y.; Wang, J.; Du, L.; Gao, Y. Differential code bias estimation based on uncombined PPP with LEO onboard GPS observations. *Advances in Space Research* **2020**, *65*, 541–551. https://doi.org/https://doi.org/10.1016/j.asr.2019.10.005.
9. Fan, X.; Du, L.; Duan, D. Synchrophasor Data Correction Under GPS Spoofing Attack: A State Estimation-Based Approach. *IEEE Transactions on Smart Grid* **2018**, *9*, 4538–4546. https://doi.org/10.1109/TSG.2017.2662688.
10. Kwon, K.C.; Shim, D.S. Performance Analysis of Direct GPS Spoofing Detection Method with AHRS/Accelerometer. *Sensors* **2020**, *20*. https://doi.org/10.3390/s20040954.
11. Basan, E.; Basan, A.; Nekrasov, A.; Fidge, C.; Sushkin, N.; Peskova, O. GPS-Spoofing Attack Detection Technology for UAVs Based on Kullback–Leibler Divergence. *Drones* **2022**, *6*. https://doi.org/10.3390/drones6010008.
12. Sharma, G.; Kushwaha, S. A Comprehensive Review of Multi- Layer Convolutional Sparse Coding in Semantic Segmentation. In Proceedings of the 2024 9th International Conference on Communication and Electronics Systems (ICCES), 2024, pp. 2050–2054. https://doi.org/10.1109/ICCES63552.2024.10859683.
13. Yang, Y.; Chen, T.; Zhao, L. From Segmentation to Classification: A Deep Learning Scheme for Sintered Surface Images Processing. *Processes* **2024**, *12*. https://doi.org/10.3390/pr12010053.
14. Kore, V.; Khadse, V. Progressive Heterogeneous Ensemble Learning for Cancer Gene Expression Classification. In Proceedings of the 2022 International Conference on Machine Learning, Computer Systems and Security (MLCSS), 2022, pp. 149–153. https://doi.org/10.1109/MLCSS57186.2022.00035.
15. Wei, X.; Sun, C.; Lyu, M.; Song, Q.; Li, Y. ConstDet: Control Semantics-Based Detection for GPS Spoofing Attacks on UAVs. *Remote Sensing* **2022**, *14*. https://doi.org/10.3390/rs14215587.
16. Bose, S.C. GPS Spoofing Detection by Neural Network Machine Learning. *IEEE Aerospace and Electronic Systems Magazine* **2022**, *37*, 18–31. https://doi.org/10.1109/MAES.2021.3100844.
17. Ren, Y.; Restivo, R.D.; Tan, W.; Wang, J.; Liu, Y.; Jiang, B.; Wang, H.; Song, H. Knowledge Distillation-Based GPS Spoofing Detection for Small UAV. *Future Internet* **2023**, *15*. https://doi.org/10.3390/fi15120389.
18. Meng, L.; Zhang, L.; Yang, L.; Yang, W. A GPS-Adaptive Spoofing Detection Method for the Small UAV Cluster. *Drones* **2023**, *7*. https://doi.org/10.3390/drones7070461.
19. Song, J.; Qu, Z.; Li, Y.; Rizos, C. A Hybrid Optimization-Based INS-Aided GNSS Spoofing Detection Method. *IEEE Transactions on Instrumentation and Measurement* **2025**, *74*, 1–12. https://doi.org/10.1109/TIM.2025.3619259.
20. Chen, T.; Zhang, J.; Li, W.; Yu, X.; Yang, Y.; Guo, L. Reliability-Guaranteed Fault Observer Design for Systems With Stochastic Parametric Uncertainty. *IEEE Control Systems Letters* **2024**, *8*, 3434–3439. https://doi.org/10.1109/LCSYS.2025.3545552.
21. Kuriş, U.; Turna, O.C. Performance Analysis of LSTM, GRU and Hybrid LSTM–GRU Model for Detecting GPS Spoofing Attacks. *Sensors* **2026**, *26*. https://doi.org/10.3390/s26041111.
22. Aissou, G. A DATASET for GPS Spoofing Detection on Unmanned Aerial System. https://doi.org/10.17632/z7dj3yyzt8.3.
23. Costa, V.G.; Pedreira, C.E. Recent advances in decision trees: an updated survey. *56*, 4765–4800. https://doi.org/10.1007/s10462-022-10275-5.
24. Shi, Y.; Lu, X.; Niu, Y.; Li, Y. Efficient Jamming Identification in Wireless Communication: Using Small Sample Data Driven Naive Bayes Classifier. *IEEE Wireless Communications Letters* **2021**, *10*, 1375–1379. https://doi.org/10.1109/LWC.2021.3064843.
25. Halder, R.K.; Uddin, M.N.; Uddin, M.A.; Aryal, S.; Khraisat, A. Enhancing K-nearest neighbor algorithm: a comprehensive review and performance analysis of modifications. *11*, 113. https://doi.org/10.1186/s40537-024-00973-y.
26. Hosmer Jr, D.W.; Lemeshow, S.; Sturdivant, R.X. *Applied logistic regression*; John Wiley & Sons, 2013.
27. Hu, J.; Szymczak, S. A review on longitudinal data analysis with random forest. *Briefings in Bioinformatics* **2023**, *24*, 559, [https://academic.oup.com/bib/article-pdf/24/2/bbad002/49559948/bbad002.pdf]. https://doi.org/10.1093/bib/bbad002.
28. Chauhan, V.K.; Dahiya, K.; Sharma, A. Problem formulations and solvers in linear SVM: a review. *52*, 803–855. https://doi.org/10.1007/s10462-018-9614-6.

 doi:10.20944/preprints202604.1124.v1

29. Chen, T.; Guestrin, C. XGBoost: A Scalable Tree Boosting System. In Proceedings of the Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, New York, NY, USA, 2016; KDD '16, p. 785–794. https://doi.org/10.1145/2939672.2939785.
30. Arik, S.O.; Pfister, T. TabNet: Attentive Interpretable Tabular Learning. In Proceedings of the Proceedings of the AAAI Conference on Artificial Intelligence, Vol. 35, pp. 6679–6687. https://doi.org/10.1609/aaai.v35i8.16826.