Journal of Systems Engineering and Electronics
Vol. 37, No. 3, June 2026, pp.1059 – 1080

Hybrid adaptive machine learning approach for detection and mitigation of GNSS spoofing through enhanced osprey optimization algorithm

KOTI Sushmitha[1,*] and SANDHYA Rachamalla[2]

1. Department of Electronics and Communication Engineering, University College of Engineering, Osmania University, Telangana Hyderabad 500007, India; 2. Department of Electronics and Communication Engineering, University College of Engineering, Osmania University, Telangana Hyderabad 500007, India

Abstract: Global Navigation Satellite Systems (GNSSs) are the specific term utilized with satellite constellation to acquire regional or global services. GNSS sensors use pseudo-distance measurement to estimate the position, velocity, and time (PVT). Several GNSS devices are exposed to detect spoofing attacks due to the use of unsafe locations. In addition, misleading signals are intentionally used to generate timing and position, and GNSS signal spoofing provides a constant risk to consumers. In past works, the implementation of the Global Positioning System (GPS) in autonomous vehicle navigation might be endangered by spoofing. To mitigate these issues, this task develops a hybrid machine-learning method for mitigating and detecting GNSS spoofing attacks. The developed model is processed with three phases: data collection, feature extraction, and detection. Initially, the required data is taken from the standard resource. Then, the data is given to the feature extraction phase. The features of the data are retrieved using the principal component analysis (PCA) and t-distributed stochastic neighbor embedding (t-SNE) model. The features obtained from the collected data are transferred to the detection phase. In the final phase, the GNSS spoofing detection and mitigation is executed using a machine learning method called as hybridized adaptive Bayesian learning and multi-layer perceptron (HABMLP). Enhanced osprey optimization algorithm (EOOA) is utilized for optimizing the variables to enhance the efficacy of models and achieves greater performance than other standard models.

Keywords: Global Navigation Satellite System (GNSS), detection and mitigation of GNSS, t-distributed stochastic neighbor embedding (t-SNE), enhanced osprey optimization algorithm, principal component analysis (PCA), hybridized adaptive Bayesian learning and multi-layer perceptron (HABMLP).

DOI: 10.23919/JSEE.2026.000124

Manuscript received July 03, 2024.
*Corresponding author.

1. Introduction

In order to offer high-precision time for financial transactions, smart power grids, and telecommunication networks, the Global Navigation Satellite Systems (GNSSs) have been deployed extensively [1]. For a wide range of military and commercial uses, the GNSS offers position, velocity, and time (PVT) data. In the commercial, military, and civil spheres, the GNSS like Global Positioning System (GPS) offers critical positioning and timing. A navigation system is highly accurate, durable, and dependable for autonomous vehicles [2]. Present automated vehicular navigation technologies mainly rely on GNSS which includes GPS receivers. However, it is the most common interference like multipath, jamming, and spoofing that affects GPS signals [3]. Due to location based services (LBS), advancements have been made for different stakeholders to share location information. Generally speaking, the best method for determining a user's location is GNSS [4]. The location data can be used to provide a variety of location-based services. The protection of privacy in LBS is frequently compromised by its users [5]. The market is flooded with GNSS standards and blueprints, which allow for a variety of GNSS sensor assaults [6]. Usually, the sources of intentional interference include the spoofer, blocker, and meta-cone [7]. A blocker is an instrument used with the same frequency noise, which prevents the GNSS receiver from collecting measurements. Due to the technological and hardware constraints on the general implementation of counter-spoofing techniques, the minimal processing-intensive approach draws inspiration from nature to combat spoofing of GNSS data [8]. By taking the temporal difference of arrival (TDOA) features between deceived and genuine signals, differential pseudo rings are taken from dif-

ferent receivers to detect spoofing [9].

A multitude of observations present in the GNSS data generated during the PVT solution can be cross-correlated to detect spoofing [10]. Due to the free access nature of GPS coarse acquisition (C/A) codes', the program may be vulnerable to malicious attacks [11]. These inadvertent efforts are known as spoofing and jamming. A more sophisticated and dangerous kind of assault called spoofing can mimic GPS signals to fool the target receiver, whereas jamming tries to weaken GPS channels by blocking or overloading signals [12]. To achieve the necessary performance in spoofing detection, graph theory and simultaneous localization of the jammer as well as a target with power difference of arrival (PDOA) are utilized [13]. Many techniques are adopted to correlate the outputs that are already utilized by the delay-locked loop (DLL) to monitor the direct signal and estimate the duration of propagation. Some of the most illustrative techniques in this class are the strobe correlator, double delta correlator, and narrow correlator approach [14]. The artificial intelligence approach is suggested for spoofing detection due to its wide advancement. A carrier-phase multipath identification framework is constructed with conventional neural networks (CNN).

Although the spoofing attack is successfully detected by the existing approaches, the PVT is not to be estimated. As a result, GNSS navigation has been a highly interesting field in recent days [15]. In fact, the multipath is distinguishable and excisable from the direct path because of its unique spectral properties [16]. Nevertheless, these techniques might harm the signal, particularly if the multipath wavelengths are closer to the direct path's spectrum. Considering the level of difficulty of the spoofing device, the spoofing assaults are categorized into three categories like simple, intermediate, and advanced. It is most economical to implement the intermediate spoofing in real time [17]. The traditional approaches developed for detecting the GNSS spoofing attack mainly rely on hardware requirements, which enhances the cost expenditure of the detection process. Moreover, the characteristics of the GNSS are considered by the conventional approaches to perform the detection process, and the time requirements of the detection process are greatly increased. An approach for GNSS spoofing identification and prevention utilizing machine learning technology is presented in order to address the aforementioned problems.

The precise contribution of the hybrid machine learning-based GNSS spoofing recognition and mitigation approach is pointed out as follows.

(i) To design the hybrid machine learning-based GNSS spoofing recognition and alleviation framework for maintaining navigation and providing accurate PVT details for civil and military services.

(ii) To suggest a feature extraction process using t-SNE and PCA for converting the high dimensional data into low dimensional data that can be used to enhance the accuracy of GNSS spoofing detection.

(iii) To provide an enhanced osprey optimization algorithm (EOOA) for tuning the constraints of the machine learning model, this process maximizes the precision and accuracy of the GNSS spoofing mitigation and detection process.

(iv) To perform the GNSS spoofing recognition and mitigation, a hybridized adaptive Bayesian learning and multi-layer perceptron (HABMLP) is suggested by hybridizing the Bayesian learning (BL) and multi-layer perception (MLP). This HABMLP considers the strength of both BL and MLP to attain better detection outcomes.

(v) To confirm the efficacy of the HABMLP-based GNSS spoofing recognition and mitigation framework by analyzing the results of the developed HABMLP with the traditional approaches using several indices.

The leftovers of this work are depicted below. Section 2 lists the existing model limitations and uses. In Section 3, the structural view of the proposed machine learning-based GNSS spoofing discovery and mitigation framework is given. The extraction of features for providing correlation among data in GNSS spoofing is provided in Section 4. The hybridized network for GNSS spoofing with its objective formulation is discussed in Section 5. The result and discussion of the HABMLP-based detection and mitigation are represented in Section 6. At last, the conclusion of HABMLP-based GNSS spoofing detection and mitigation is given in Section 7.

2. Literature survey

2.1 Related works

In 2019, Meng et al. [18] suggested a spoofing generator based on a software-defined receiver (SDR) with vector tracking. In 2019, Semanjski et al. [19] developed an intelligent technique to identify possibly manipulated GNSS signals by tracking the cross-correlation of several GNSS measurements. In 2022, Shang et al. [20] developed a brand-new time synchronization attacks (TSA) mitigation algorithm based on a single antenna. Initially, the parameters of the real and fake signals were determined using a multi-correlator estimator. In 2021, Singh et al. [21] explored a cutting-edge method for spoofing attack detection and mitigation. To implement the suggested algorithm in the Android application, the OpenStreetMap dataset are considered. In 2020, Schmidt et

al. [22] suggested an approach for identifying and classifying GNSS spoofing in single-antenna receivers. In order to reduce false alerts, the researcher applied a threshold. In 2022, Pardhasaradhi et al. [23] suggested the extended Kalman filter (EKF) architecture, which is utilized by the GNSS receivers to estimate their PVT. In 2022, Blais et al. [24] put forth a unique framework for GNSS multipath prediction. The process was initiated by creating datasets that are processed by the CNNs. Grayscale 2D images were created by mapping correlations between the local replica grid and the received signal. In 2023, Nayfeh et al. [25] gave a developed model for the identification and categorization of unmanned aerial vehicle (UAV) GPS spoofing.

2.2 Problem statement

Due to the broad application, GNSS has presently grown and requires the minimum cost. The occurrence of GNSS is used in phased measurement unit (PMU), emergency service, power grid, and financial transactions. The spreading of GNSS receivers in smart cars and phones allows the general to have access to our localization. Moreover, the position quality determined by the GNSS equipment minimizes based on the received signals. This form of degradation is formed to find the signal generation system. SDR [18] has the capacity to track the original code accurately in the urban environment. It easily changes the spoofing into carrier or code but requires a mature vector tracking framework. Support vector machine (SVM) [19] has the maximum capacity in helping the GNSS signal spoofing detection and is also performed under huge datasets. However, it has slight variation in the validation result. The TSA mitigation process [20] requires only a single antenna and is cost-effective. However, it has the chance to form false time information while transmitting signals. Genetic algorithm [21] has the capacity to escape from local optimal problems, but it is computationally more expensive. Least absolute shrinkage and selection operator (LASSO) [22] supports for enhancing the automatic peak discrimination and generates robust outcomes. However, it requires an optimization algorithm to solve the computational requirement. The generalized likelihood ratio test (GLRT) [23] helps to identify the spoofing attack and attains the optimal rate of overall analysis. However, it requires recalculation for accurate results. CNN [24] has high multipath detection power and takes less time for parameter estimation. However, it requires data features in prior. Machine learning (ML) [25] gives a solution for detecting GPS spoofing and supports in identifying real-time detection. However, it takes more time and resources. Therefore, to solve the difficulties, this paper proposed the ML technique for detecting spoofing in the GNSS framework.

3. Methods

3.1 Challenges during GNSS spoofing detection and mitigation

The intellectual transference system and the locality-aided services are successfully operated and implemented in the market by the PVT application. The PVT effectively attains the information via the GNSS. However, the GNSS is highly susceptible to several types of attacks. The spoofing is the most common attack in the GNSS system. In this process, the authentic GNSS signals are alleviated by the spoofer and convey the wrong information to the victim. In order to make the safe navigation process, GNSS spoofing detection is necessary. The conventional GNSS spoofing detection approaches require too much cost for the spoofing detection process. Moreover, the existing approaches for detecting GNSS spoofing are not suited for large-scale deployment. The GNSS spoofing attack can occur at any time and place within a limited period of time, which cannot be monitored by the existing approaches. The existing model does not identify the spoofed signal that may provide wrong data to civil and military applications. The conventional techniques for spoofing attack detection do not identify the presence of a spoofer along the quality of the signal cannot be monitored by the traditional techniques. Further, the existing approaches utilize the autocorrelation function to identify the spoofed signal, which may raise the time required for the GNSS spoofing. The planned and the inadvertent interference in the GNSS are not identified by the traditional approaches. The power level fluctuation in the GNSS signal is not handled by the traditional techniques. Moreover, the hardware requirement for the GNSS spoofing is quite high for the traditional approaches. To counter the challenges of the traditional approaches, the hybrid ML approach is developed for the GNSS spoofing.

3.2 Structural view of proposed model

A hybrid GNSS spoofing detection and mitigation framework is developed to find the spoofing signal in the GNSS and mitigate it to offer PVT services for civil and military services. Moreover, the developed model is applied in the GNSS receiver to find and eliminate the false signal induced by the spoofer to provide proper navigation in the country [26]. Besides, the suggested ML system identifies the attack modes of the spoofer and its corresponding properties with fewer hardware requirements [27]. In order to begin the GNSS spoofing detec-

tion and mitigation process, the needed data are taken from online sources. Further, the collected data is subjected to the feature extraction procedure. The feature of the data is retrieved using two approaches like t-SNE and the PCA. The feature extraction enhances the spoofing detection efficiency of the ML methods. The high-dimensional data is converted into the lower-dimensional data with the help of the t-SNE. Moreover, the most significant features in the data are represented using the t-SNE structure. Similarly, the PCA approaches extract the principal components that are called as features and it is available in more understandable form. The features attained from the t-SNE and PCA are integrated and passed to the HABMLP. The HABMLP is formed by integrating the two machine learning structures BL and MLP. Both of the hybrid structure works together and produce higher accuracy in the GNSS spoofing detection and mitigation process. Both BL and MLP examine the features obtained from the t-SNE and PCA to get accurate results. Here, the BL model adopts the Bayes rule [28] to get the detection result and similarly, the MLP structure analyses the features using its complex layer. During this process, the suggested EOOA optimizes the hidden and epoch count of the BL as well as the steps per epoch of MLP to obtain the accurate prediction result. Once the HABMLP detects the GNSS spoofing, the mitigation process is executed by the same HABMLP, here the alarm is produced as a warning sign once the spoofer can tamper the GNSS signal. To this end, the experimental analysis is performed on the output of the developed hybrid ML-based structure to confirm its effectiveness. The structural representation of the HABMLP-based GNSS spoofing recognition and mitigation framework is illustrated in Fig. 1.

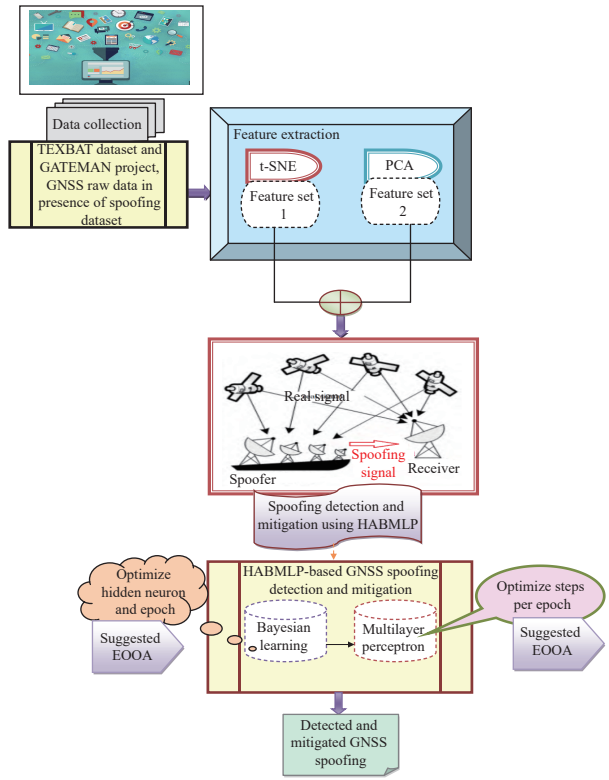


Fig. 1 Hybrid ML-based GNSS spoofing detection and mitigation framework

3.3 Dataset used

The dataset utilized in the GNSS spoofing attack detection and mitigation approach is elaborated in the below section. Here, the collected dataset is used to validate the GNSS spoofing framework performance. The consideration of these datasets splits into two equal halves and it represents datasets 1 and 2 according to the collected data. This dataset considers publicly available data. The detailed description of this dataset is mentioned below.

Dataset 1 & Dataset 2: Galileo open service navigation message authentication (FGI OSNMA) datasets are taken from the link of https://etsin.fairdata.fi/dataset/09dc5c1b-933d-4efd-aa66-be2c07fab3b3/data with access: 2024-04-09. Galileo E1 and GPS L1 C/A signals in raw GNSS in-phase and quadrature (I/Q) data are presented in this dataset. Stereo-dual-band GNSS front-end is used to gather I/Q data samples. The open sky in this dataset helps to examine the performance of OSNMA at no spoofing condition. The position of this dataset is calculated by 60.182°N, 24.828°E geodetic grade receiver with 47.248 m altitude. The collected data is regenerated with LabSat wide-band 3 and captured through the GNSS front-end. This dataset is highly important to validate the OSNMA-based spoofing detection effectiveness in a real-world scenario. The actual data for datasets 1 and 2 is shown in Table 1.

Table 1 Actual data representation for dataset 1 and dataset 2 in GNSS spoofing attack detection and mitigation

Dataset	Channel 1	Channel 2	Channel 3	Channel 4	Channel 5	Channel 6	Channel 7	Channel 8	Channel 9	Channel 10
Dataset 1	0.00096	0.02603	0.00733	0.03139	0.01747	0.03151	0.00083	0.03093	0.03620	0.02802
	0.00012	0.02721	0.00718	0.03351	0.01747	0.03517	0.00236	0.03270	0.00045	0.02995
	0.03889	0.02842	0.00685	0.03488	0.01752	0.03870	0.00342	0.03438	0.00414	0.03177
	0.03797	0.02962	0.00666	0.03649	0.01750	0.00311	0.00455	0.03618	0.00767	0.03389

Continued

Dataset	Channel 1	Channel 2	Channel 3	Channel 4	Channel 5	Channel 6	Channel 7	Channel 8	Channel 9	Channel 10
Dataset 1	0.03729	0.03090	0.00635	0.03835	0.01755	0.00676	0.00582	0.03795	0.01120	0.03565
	0.03651	0.03219	0.00607	0.00071	0.01766	0.01047	0.00707	0.00031	0.01483	0.03706
	0.03628	0.0334	0.00606	0.00257	0.01772	0.01391	0.00837	0.00155	0.01833	0.03865
	0.03544	0.03469	0.00578	0.00426	0.01772	0.01760	0.00927	0.00330	0.02187	0.00112
	0.03389	0.03587	0.00563	0.00611	0.01782	0.02139	0.01040	0.00515	0.02548	0.00316
	0.03345	0.03712	0.00531	0.00783	0.01792	0.02495	0.01178	0.00687	0.02901	0.00488
Dataset 2	0.01009	0.03524	0.00851	0.00959	0.01030	0.00591	0.03217	0.00612	0.00981	0.03710
	0.01128	0.03514	0.00978	0.00802	0.01144	0.00835	0.03478	0.00989	0.00961	0.03873
	0.01245	0.03493	0.01077	0.00700	0.01259	0.01079	0.03715	0.01353	0.00953	0.00100
	0.01363	0.03482	0.01201	0.00592	0.01369	0.01322	0.00052	0.01752	0.00940	0.00261
	0.01479	0.03464	0.01311	0.00491	0.01480	0.01568	0.00305	0.02124	0.00923	0.00427
	0.01593	0.03454	0.01387	0.00375	0.01591	0.01809	0.00536	0.02456	0.00903	0.00590
	0.01708	0.03442	0.01498	0.00310	0.01701	0.02056	0.00798	0.02839	0.00870	0.00749
	0.01827	0.03435	0.01632	0.00187	0.01813	0.02305	0.01067	0.03215	0.00858	0.00919
	0.01943	0.03425	0.01756	0.0008	0.01926	0.02548	0.01332	0.03554	0.00843	0.01086
	0.02060	0.03407	0.01896	0.03927	0.02038	0.02795	0.01612	0.03918	0.00821	0.01243

The parameters utilized in the hybrid ML-based GNSS spoofing detection and mitigation framework are elucidated in Table 2.

Table 2 Variables utilized in the proposed model

Parameter	Detail
Batch size in KNN	48
Effective metric in KNN	Euclidean
Activation function in MLP	ReLu
Learning rate in MLP	0.01
Epochs in MLP	100
Batch size in BL	64
Activation function of HABMLP	ReLu
Batch size in HABMLP	64
Learning rate in HABMLP	0.01
Epochs in HABMLP	100

The gathered data from the online resources is represented as G_m^r and $m = 1, 2, \cdots, M$, here, the total quantity of the gathered data from the online resources is represented as M.

3.4 Brief elucidation of proposed EOOA

The EOOA is a new optimization algorithm, which is modeled from the baseline osprey optimization algorithm (OOA) [29] by upgrading the random parameter. It is suggested to maximize the efficacy of the hybridized expert systems in the GNSS spoofing recognition and mitigation process. The parameters of the BL and MLP are optimized by the EOOA to enhance the precision and accuracy of the developed model. The explored EOOA optimizes the steps per epoch of the MLP as well as the number of epochs and epoch count of the BL to achieve effective performance in the GNSS spoofing detection and mitigation process. The OOA is the meta-heuristic algorithm and it is intended to consider the simulation activities of the OOA [30]. The factual world optimization trouble is solved by the OOA. At the time of the searching process, the exploitation and the exploration phases can be handled by the OOA. The convergence and the precision rate of the OOA are very poor. Additionally, the control engineering concerns are not solved by the OOA [31], and the time consumption of the OOA while maintaining the balance between the exploitation and the exportation phase is too high. Considering the above hitches, the new EOOA is developed. The accuracy and precision of the GNSS spoofing and mitigation model are enhanced using the EOOA. The worst, and best fitness and the number of population O play the most crucial role for upgrading the random number $s_{j,k}$. The mathematical term for calculating the random number $s_{j,k}$ is provided as follows:

$$s_{j,k} = \frac{(b_t)^{\frac{3}{2}} / w_t}{O} \tag{1}$$

where the random number is indicated as $s_{j,k}$. The best and worst fitness is denoted as b_t, and w_t, the number of

population is elucidated as O. The developed EOOA solves the control engineering concerns and convergence as well as the precision rate is also enhanced by the new EOOA. Further, the accuracy and the precision rate of the GNSS spoofing are enhanced by the new EOOA.

The pseudocode of the EOOA is stated in Algorithm 1.

Algorithm 1 Developed EOOA

Start
Provide the constraints and parameters
Fix the count of population O and iteration value U
Initialize the population matrix and objective function
For $j = 1$ to O
Upgrade the random number by (1)
Phase 1
  Modernize the location of the fish
  Find the novel location of the jth OOA member
  Verify the boundary condition of OOA
  Upgrade the jth OOA
Phase 2
  Find the jth OOA member
  Verify the edge condition of OOA
  Upgrade the jth OOA
  Store the excellent solution
End for
Stop

4. Extraction of features for providing correlation among data in GNSS spoofing

4.1 t-SNE

The size of the entire data is condensed by the powerful technique called as t-SNE. The t-SNE is used to analyze the gathered data's structure. If the linear boundary of the collected data is too complex, the t-SNE is adopted which analyzes the entire data point and retrieves the most important feature. The collected data G_m^r is given into the t-SNE [32] for obtaining the relevant features from the data. The t-SNE is used to take out the feature from the collected data. The t-SNE has a high multi-dimensional scaling property. The t-SNE is applied between the data points of the gathered data to project the Euclidean distance among those points. The coordination between the data points y_k and y_j is identified with the aid of conditional probability $Q_{k|j}$ and it is represented as follows:

$$Q_{k|j} = \frac{\exp(-\left\|y_j - y_k\right\| / 2\wp_j^2)}{\sum_{j \neq l} \exp(-\left\|y_j - y_k\right\| / 2\wp_j^2)}. \tag{2}$$

In the original feature space, this probability is arithmetically signified as indicated as follows:

$$Q_{j,k} = \left(\frac{Q_{j|k} + Q_{k|j}}{2o}\right). \tag{3}$$

Thus, the dimension of the data is represented as o, the vicinity of the data points is identified with the help of the perplexity constant in the t-SNE and it is expressed as follows:

$$\text{Perplexity}(Q_j) = 2^{I(Q_j)} \tag{4}$$

where $I(Q_j)$ is the Shannon entropy.

The pairwise distance between the data points can be used to adjust the variance $\wp_j$. Similarly, the low dimensional probability r_{jk} can be expressed as follows:

$$r_{jk} = \frac{(1 + \|n_j - n_k\|^2)^{-1}}{\sum_{j \neq k} \left(1 + \|n_j - n_k\|^2\right)^{-1}}. \tag{5}$$

The input data y_j can be converted into lower dimensional data n_j with the aid of t-SNE. The data can be effectively visualized with the help of the t-SNE. The features obtained from the collected data G_m^r using t-SNE are denoted as d_m^{tsne}.

4.2 PCA-based features

The principal component analysis (PCA) [33] approach reduces the dimension of the data and converts it into a lower dimension by projecting the data in a geometric way. The features obtained from the PCA are very easy to learn so it gives accurate results. The relevant features from the gathered data are hauled out using the PCA [33]. From the set of data, the dominant features also called as principal components are extracted using the technique named as PCA. The data are projected on the ortho-usual subspace by applying the linear transform. The collected data can be minimized by the PCA and very useful information for the spoofing process is available in the retrieved features [34]. The collected data is converted into a column vector ν_o in order to attain the Eigen data. Based on the utilization of the variables, the length of the column vector is varied. The matrix array ν with the dimension of $N \times O$ is developed for the input observation N and it is given as follows:

$$\boldsymbol{\nu} = [\nu_1, \nu_2, \nu_3 \cdots \nu_N]. \tag{6}$$

The average data κ is represented as follows:

$$\kappa = \frac{1}{N} \sum_{o=1}^{N} \nu_o. \tag{7}$$

The average data and the training data are subtracted to

get the difference data and it is represented as follows:

$$\vartheta_j = \nu_j - \kappa. \tag{8}$$

Later, the orthogonal Eigenvector and covariance D of the PCA is identified and it is stated as follows:

$$D = \frac{1}{N}\sum_{o=1}^{N} \boldsymbol{\vartheta}_o \cdot \boldsymbol{\vartheta}_o^{\mathrm{T}} = \frac{1}{N}\boldsymbol{B}\cdot\boldsymbol{B}^{\mathrm{T}}, \tag{9}$$

$$\boldsymbol{B} = [\vartheta_1, \vartheta_2, \cdots, \vartheta_N]. \tag{10}$$

The computation process can be lowered by considering the Eigenvector represented as w_j.

$$\boldsymbol{B}^{\mathrm{T}} \cdot \boldsymbol{B} w_j = \beta_j w_j \tag{11}$$

The Eigenvector of the covariance D can be identified by

$$\boldsymbol{v}_j = \boldsymbol{B} w_j, \tag{12}$$

$$\boldsymbol{D} = \boldsymbol{B} \times \boldsymbol{B}^{\mathrm{T}}, \tag{13}$$

where the Eigen data is represented as v_j. Based on the large Eigenvalue, the required Eigen data N could be selected. For any data, the principal component is defined as follows:

$$x_l = \boldsymbol{v}_l^{\mathrm{T}}(\boldsymbol{\nu} - \kappa \boldsymbol{I}). \tag{14}$$

Based on the Eigenvector, the value x_l can be mapped with the axis. The values are signified as the feature of the data that can be employed in the spoofing detection process. The features from the PCA are represented as d_m^{pca}.

Both of these feature like d_m^{tsne} and d_m^{pca} are fused and it is passed to the HABMLP for spoofing detection and mitigation process. Here, the fused feature is termed as d_m^{com}.

5. Hybridized ML network for GNSS spoofing with its objective formulation

5.1 BL model

The BL model performs the detection process effectively on a limited amount of data. The fused feature d_m^{com} is passed to the BL to achieve the first detection score. The learning process of the BL is very simple as compared to another model. The BL [35] is used to find the spoofing in GNSS. The feature obtained from the t-SNE and PCA is given to the BL for getting the first detection result. The BL works on the basis of belief revision. The previous belief can be updated if any new data is available in the network. In Bayesian learning, the learning issues are considered as Bayesian probabilistic interference. For the casual model, the hypothesis space I and the data e can be developed by the learner [36]. Later, the degree of belief can be expressed by computing the subsequent probability distribution and it is represented as $Q(i|e)$. Based on the availability of the data and likelihood $Q(e|i)$, the prior probabilities $Q(i)$ can be identified. According to the Bayes rule, the multiplication of the likelihood and the prior is directly proportional to the subsequent probabilities and it is expressed as follows:

$$Q(i|e) = \frac{Q(e|i)\,Q(i)}{\sum_{i'} Q(e|i')\,Q(i')}. \tag{15}$$

The term i indicates the hypothesis and the alternative hypothesis is signified by the term i'. The detection result from the BL is denoted as S_m^{bl}. The pictorial delineation of the BL is presented in Fig. 2.

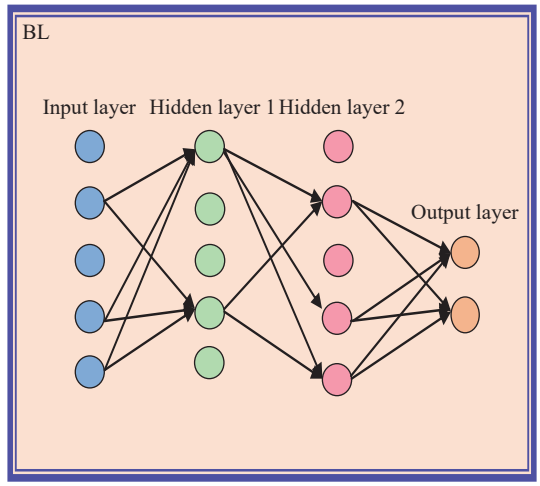


Fig. 2 Pictorial representation of BL

5.2 MLP model

The MLP analyzes the vectors of the feature to get an accurate detection result. In MLP, the value of false alarms is lower. This structure is used for GNNS spoofing detection. The fused feature d_m^{com} is given to the MLP to get the second detection score. The MLP [37] is one type of neural network and it is used to employ the spoofing detection process. The complex neuron structure of the brain is the main inspiration behind the development of MLP. It can be mathematically expressed as follows:

$$Z_l(y) = g\left\{\sum (x_{lj} y_j) + c_l\right\} \tag{16}$$

where the variable g presents the commencement function, the input layer of the jth neuron is presented as y_j, the lth perceptron output is represented as Z_l for the jth row and the lth column of the neuron; the weight matrix is denoted as $\boldsymbol{x}_{lj}$, and for the layer l, the bias value is denoted as c_l.

The loss function can be used to lower the prediction error of the MLP. The weights of individual layers can be iteratively enhanced to lower the occurrences of detection errors. The detection error is calculated at each iteration during the training process [38]. The weight and the bias are adjusted to back-propagate the error in the MLP. The loss function of the MLP can be identified as follows:

$$\mathrm{MG} = -\frac{1}{E}\sum_{j=1}^{E} z_j \cdot \ln \hat{z}_m + (1-z_j)\cdot \ln(1-\hat{z}_m). \tag{17}$$

Thus, for the data E, the jth flow of label is represented as z_j, and the mth predicted prospect of spoofing is represented as $\hat{z}_m$. The detection result obtained from the MLP is denoted as S_m^{MLP}. The pictorial visualization of the MLP is indicated in Fig. 3.

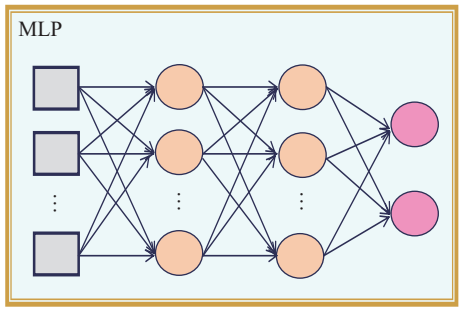


Fig. 3 Pictorial representation of MLP

5.3 Proposed HABMLP network for GNSS spoofing detection and mitigation

The HABMLP is developed for the GNSS spoofing detection and mitigation process. In HABMLP, BL and MLP are hybridized to get the accurate detection result. The hybridization process is mainly used to adapt the strength of both BL and MLP in the GNSS spoofing detection and mitigation process. The BL works on the basis of the Bayes rule to get an accurate detection result. The learning capacity of the BL is very well and it can function effectively for a limited amount of data. Likewise, the MLP is a complex brain-like structure so it deeply analyzes the vectors of the features to get the accurate detection result. The detection accuracy of hybrid ML is high. The feature from the PCA and t-SNE is fused and it is given to the BL. The BL identifies the GNSS spoofing by analyzing the nature of the signal. During the GNSS spoofing, the probability values are used to train the BL. Based on the probability of existence, the properties of the GNSS signal is identified. Likewise, in the MLP, the signal space is mapped with the input layer of the MLP. Further, the hidden layer of the MLP processes the features and conveys it into the output layer. Here, the MLP detects the GNSS spoofing by collecting the fresh GNSS signal. The output layer compares the properties of the new GNSS signal and existing information to find the presence of spoofing. The detection result from the BL and MLP is averaged to get the final detection result. At the time of the GNSS spoofing detection, the EOOA is applied to fine-tune the attributes to improve the accuracy and precision value.

Once the GNSS spoofing is detected, the GNSS mitigation is carried out, here, the alarm is created in terms of a warning signal when the spoofer is entered into the GNSS and it refreshes the GNSS receiver to its initial state. The developed HABMLP-based spoofing detection cum mitigation model is used to maintain secure navigation and it can be used to provide correct PVT to civil and military applications. The objective function of the HABMLP-based spoofing detection and mitigation model is given as follows:

$$d = \underset{\{K_c^{bl}, H_n^{bl}, N_d^{mlp}\}}{\arg\min} \left(\frac{1}{\text{accuracy}} + \frac{1}{\text{precision}} \right) \tag{18}$$

where the purpose function is represented as d, the term K_c^{bl} in $[5,255]$ represents the count of BL's hidden neuron, the steps per epoch of MLP is denoted as N_d^{mlp} in $[100,500]$ and the epoch count of BL is expressed as H_n^{bl} in $[5,50]$. The precision and accuracy rates are determined from

$$\text{accuracy} = \frac{t+g}{t+g+y+h} \tag{19}$$

and

$$\text{precision} = \frac{g}{t+y}, \tag{20}$$

where the true and false positives are delineated as t and y correspondingly. The negative and true are expressed as h and g. The structural view of the HABMLP network for GNSS spoofing recognition and mitigation is signified in Fig. 4.

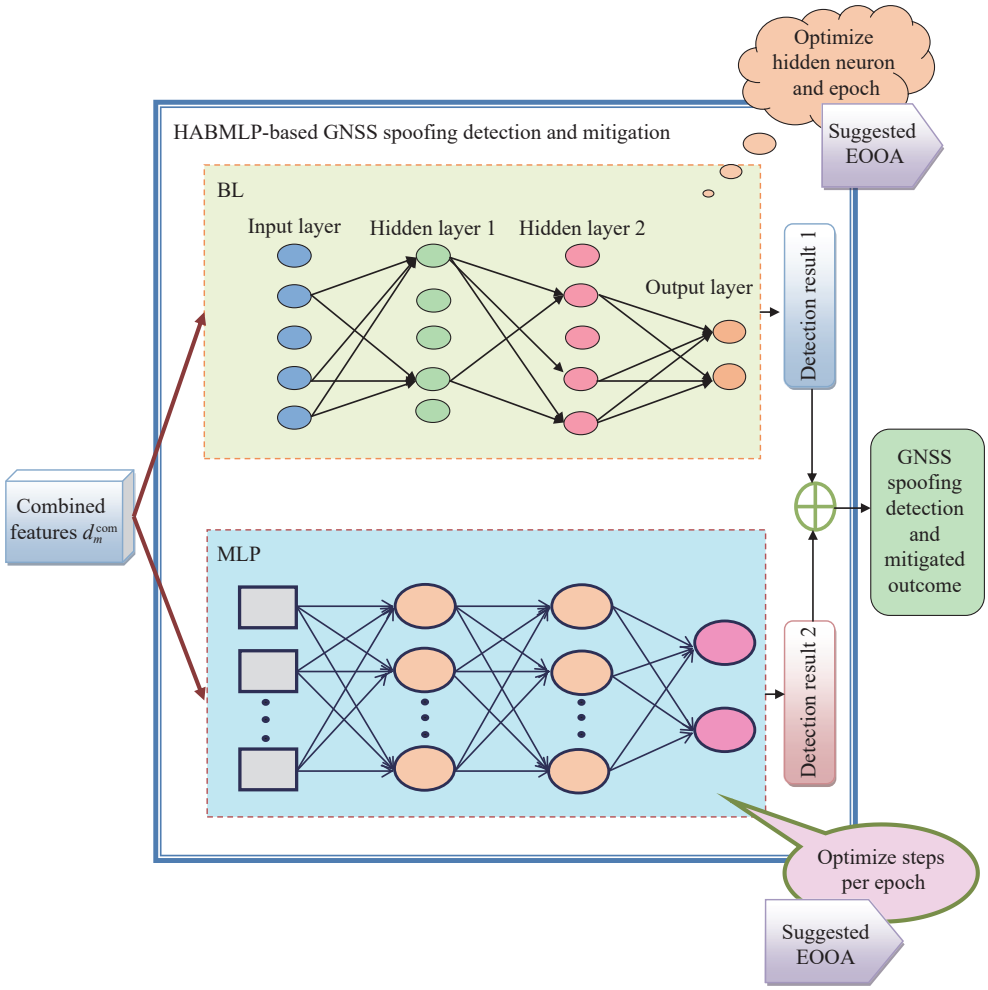


Fig. 4 Structural view of HABMLP network for GNSS Spoofing detection and mitigation

6. Result and discussion

6.1 Experimental preparation

The developed HABMLP-based GNSS spoofing attack recognition and alleviation approach is implemented using Python software. In this analysis process, chromosome length, maximum number of iterations, and population number are taken as 50, 3, and 10. In addition, the evaluation processes consider the existing algorithms like rat swarm optimizer (RSO) [39], dwarf mongoose optimization (DMO) [40], coronavirus herd immunity optimizer (CHIO) [41], OOA [29] and the traditional approaches such as K-nearest neighbour (KNN) [42,43], BL [35,44] and MLP [37,45] for verifying the efficacy of the suggested HABMLP-based GNSS spoofing attack detection and mitigation approach. The hardware requirements of the developed suggested HABMLP-based GNSS spoofing attack recognition framework are represented in Table 3.

Table 3 Hardware details of the developed method

Hardware	Size/version
RAM	8 GB
ROM	256 GB
Preprocessor	Core I3

6.2 Simulation indices

The simulation indices in the HABMLP-based GNSS spoofing attack detection and mitigation approach are listed as follows:

$$\mathrm{MCC} = \frac{t \cdot g - y \cdot h}{\sqrt{(t+y)(t+h)(g+y)(g+h)}}, \tag{21}$$

$$\mathrm{FNR} = \frac{g}{g+h}, \tag{22}$$

$$\mathrm{FDR} = \frac{y}{y+g}, \tag{23}$$

$$\mathrm{FPR} = \frac{t}{y+g}, \tag{24}$$

$$\text{NPV} = \frac{g}{g+h}, \tag{25}$$

$$\text{F1-score} = \frac{2t}{2t+y+h}, \tag{26}$$

$$\text{sensitivity} = \frac{t}{t+y}, \tag{27}$$

$$\text{specificity} = \frac{g}{g+y}. \tag{28}$$

6.3 ROC curve

The ROC curve examination of the EOOA-HABMLP-based GNSS spoofing recognition and alleviation model for dataset 1 and dataset 2 is shown in Fig. 5(a) and Fig. 5(b). The overall efficacy of the EOOA-HABMLP model in the spoofing detection and mitigation process is identified by the ROC investigation. For the second dataset, the suggested EOOA-HABMLP-based GNSS spoofing discovery and mitigation model attains the true positive rate of 8.16%, 8.1%, 6.12%, and 5.91% enhanced than the KNN, SVM, BL, and MLP at the false positive rate 0.4. Therefore, the performance of the EOOA-HABMLP-based method is better than the other baseline approaches.

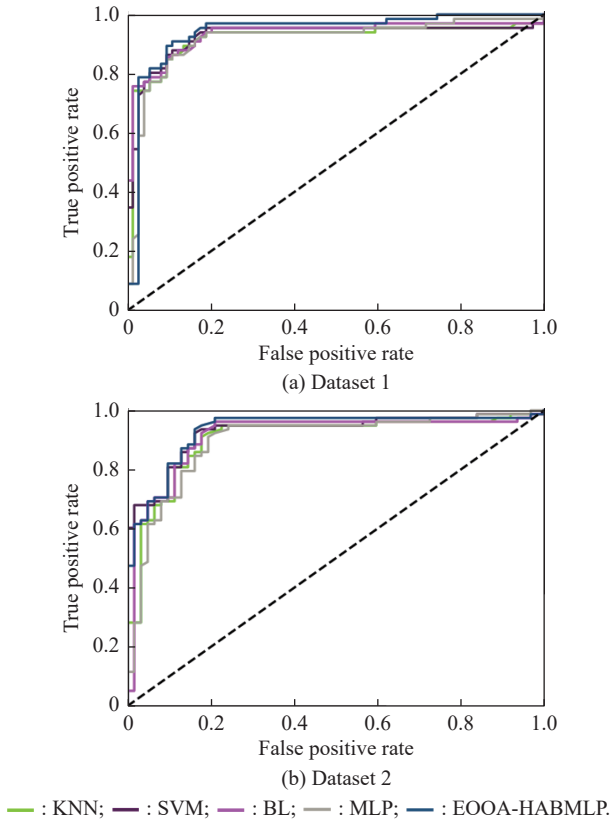


Fig. 5 ROC assessment of the hybrid ML-based model

6.4 Analysis of confusion matrix

Fig. 6(a) and Fig. 6(b) shows the confusion matrix analysis of the HABMLP-based GNSS spoofing attack detection and mitigation approach for dataset 1 and dataset 2. The developed EOOA-HABMLP method performance is summarized through the confusion matrix in terms of matrix form. From the confusion matrix analysis, the overall accuracy of the HABMLP-based GNSS spoofing attack detection and mitigation approach is acquired as 94.65% for the first dataset and 94.33% for the second dataset.

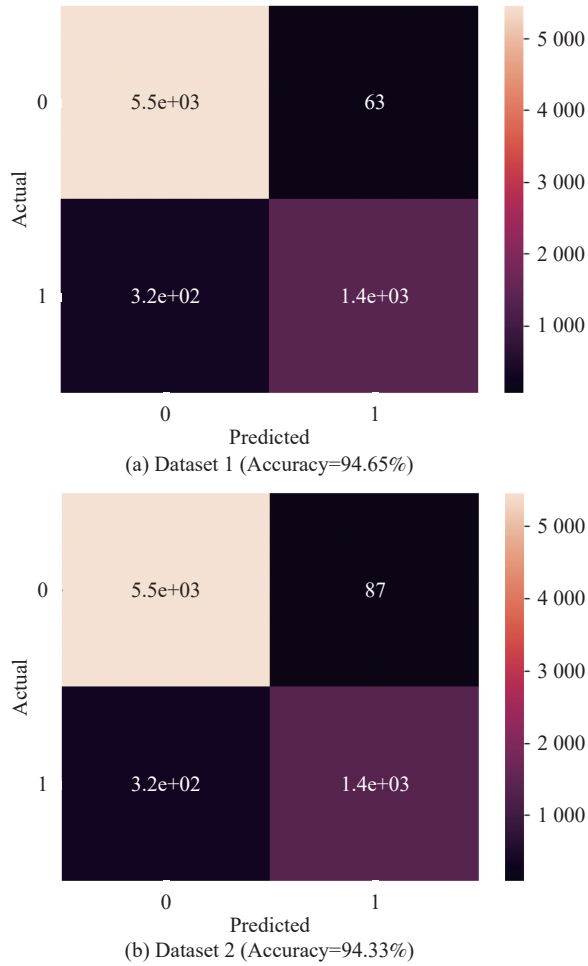


Fig. 6 Confusion matrix of the hybrid machine learning-based GNSS spoofing detection and mitigation model

6.5 Convergence analysis

Fig. 7(a) and Fig. 7(b) represents the convergence assessment of the explored EOOA-HABMLP-based model for dataset 1 and dataset 2. In the second dataset, the suggested model's cost function is lower than the RSO-HABMLP, DMO-HABMLP, CHIO-HABMLP, and OOA-HABMLP with 87.5%, 12.5%, 75% and 11.25% at the 20th iteration. Thus, the cost consumption of the EOOA-HABMLP-based method is lower than the existing approaches.

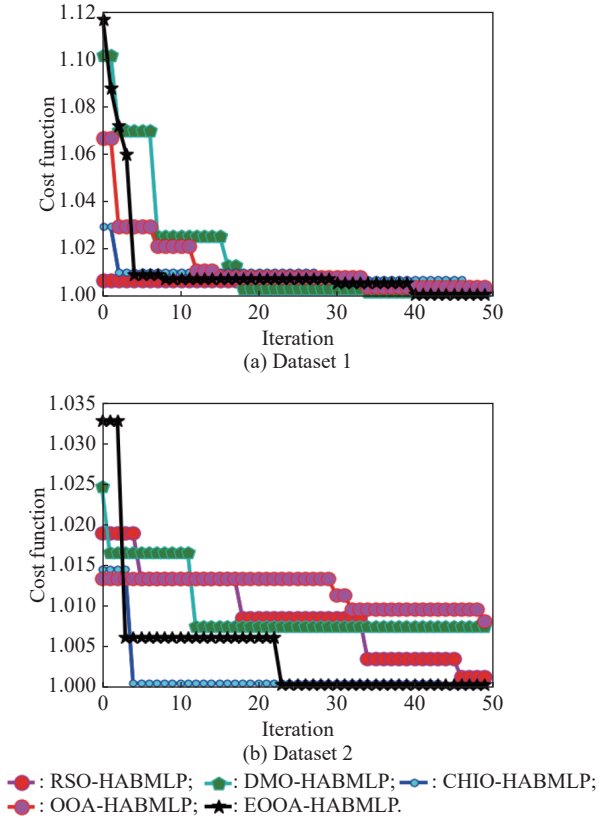
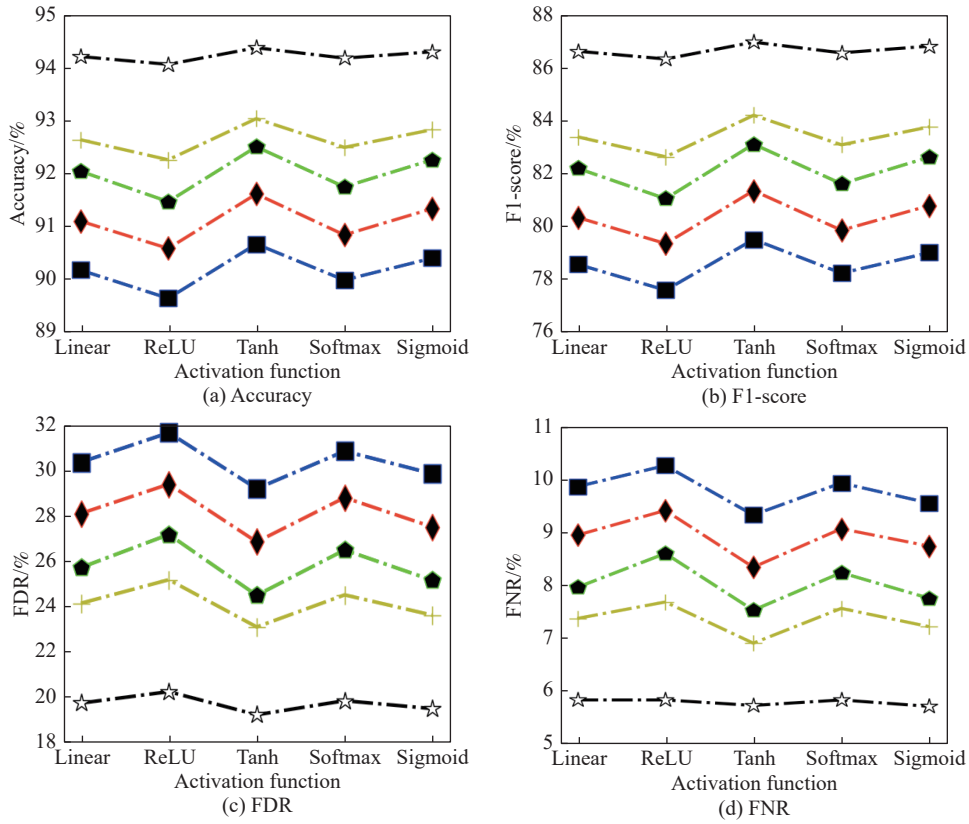


Fig. 7 Convergence assessment of the hybrid ML-based GNSS spoofing detection and mitigation mode

6.6 Algorithmic validation of the developed framework

The algorithmic assessment of the implemented EOOA-HABMLP-based GNSS spoofing detection and mitigation model for the dataset 1 in terms of accuracy, F1-score, FDR, FNR, FPR, NPV, FPR, Precision, Recall, and Specificity is illustrated in Fig. 8(a)−Fig. 8(j). Here, the population count varies in the X axis for accurately determining the efficacy variation of the implemented method with the existing mechanisms. The algorithmic assessment of the implemented model for the dataset 2 in terms of accuracy, F1-score, FDR, FNR, FPR, NPV, FPR, Precision, Recall, and Specificity is illustrated in Fig. 9(a)−Fig. 9(j). In the second dataset, the accuracy of the EOOA-HABMLP-based GNSS spoofing detection and mitigation model is higher than the RSO-HABMLP, DMO-HABMLP, CHIO-HABMLP, and OOA-HABMLP with 5.69%, 5.18%, 5.69% and 3.14% at the 6th population value for the 1st dataset. Likewise, the type II indices like FNR and FDR of the explored EOOA-HABMLP-based GNSS spoofing detection and mitigation model are lower than other traditional frameworks. Therefore, the EOOA-HABMLP-based GNSS spoofing detection and mitigation model performance is better than the traditional algorithms.



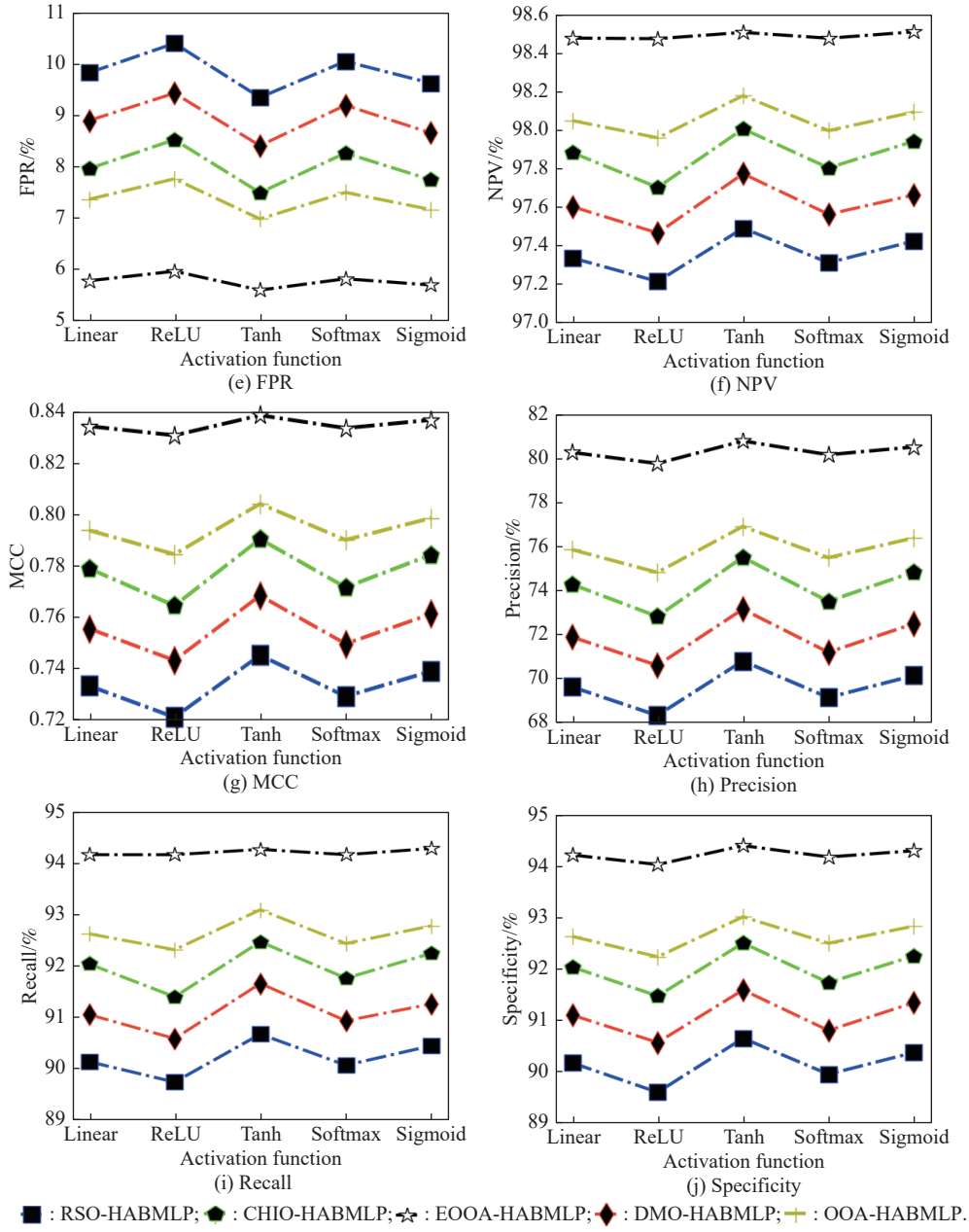
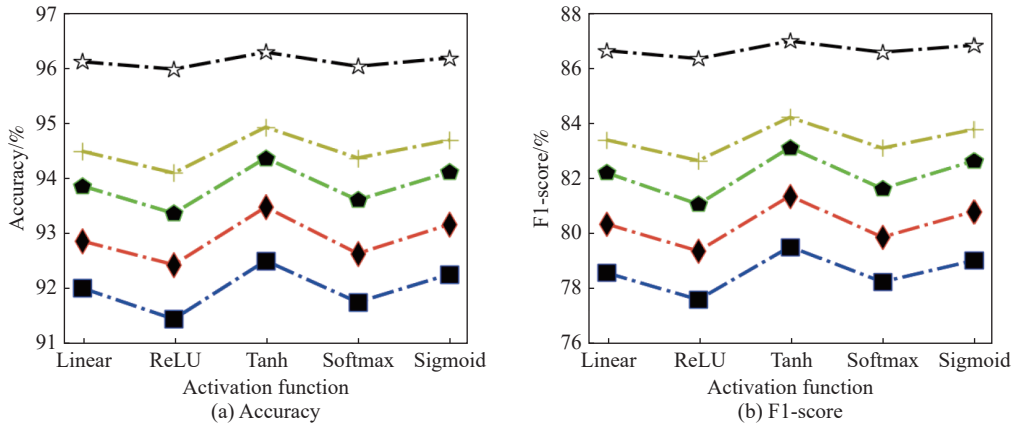


Fig. 8 Algorithmic assessment of the hybrid machine learning-based model for dataset 1



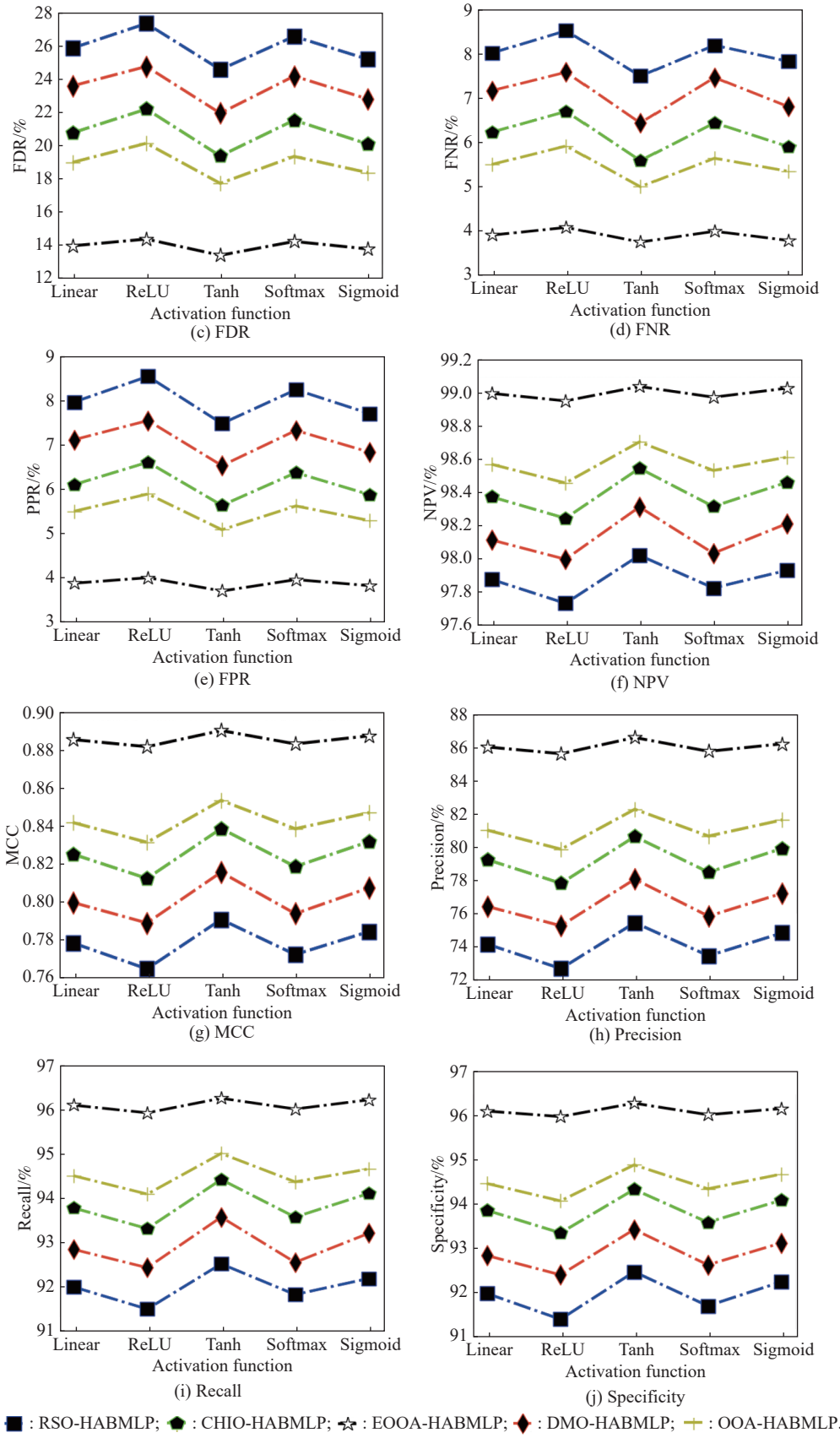
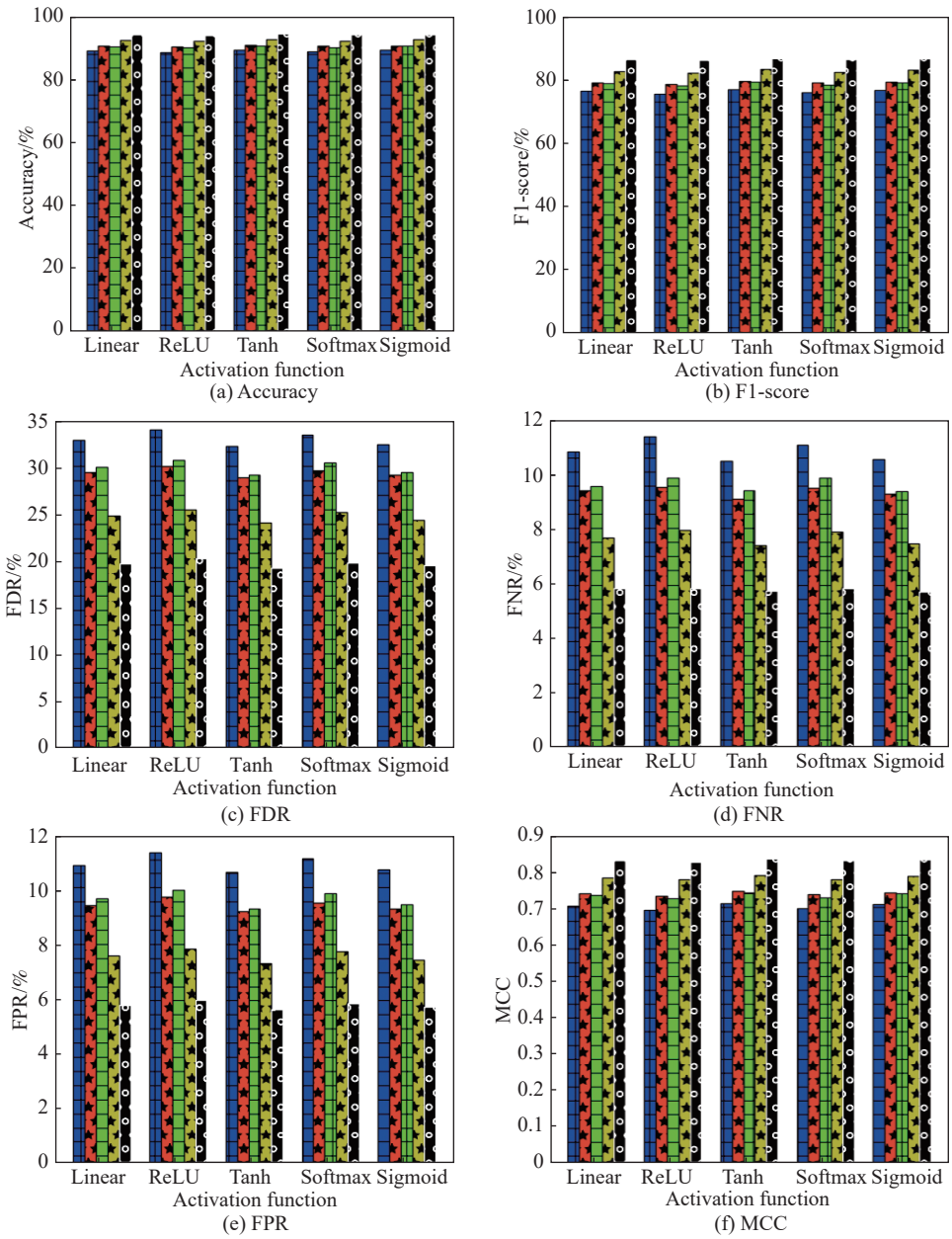


Fig. 9 Algorithmic assessment of the hybrid machine learning-based model for dataset 2

6.7 Detection techniques comparison of the explored model

The developed EOOA-HABMLP-based GNSS spoofing detection and mitigation method is compared with the baseline detection method for the dataset 1 in terms of accuracy, F1-score, FDR, FNR, FPR, NPV, FPR, Precision, Recall, and Specificity is illustrated in Fig. 10(a)−Fig. 10(j). In addition, the developed method is compared with the baseline detection method for the dataset 2 in terms of accuracy, F1-score, FDR, FNR, FPR, NPV, FPR, Precision, Recall, and Specificity is illustrated in Fig. 11(a)−Fig. 11(j). At the second dataset, the developed EOOA-HABMLP-based GNSS spoofing detection and mitigation model accomplished the MCC value of 21.73% enhanced than KNN, 13.04% enhanced than SVM, 11.9% enhanced than BL and 8.69% at tanh activation function. On the contrary, the other indices like accuracy, F1 score, and NPV of the EOOA-HABMLP-based GNSS spoofing detection and mitigation model are higher than the existing methods. Therefore, it proves the efficacy of the EOOA-HABMLP in the GNSS spoofing detection and mitigation process.



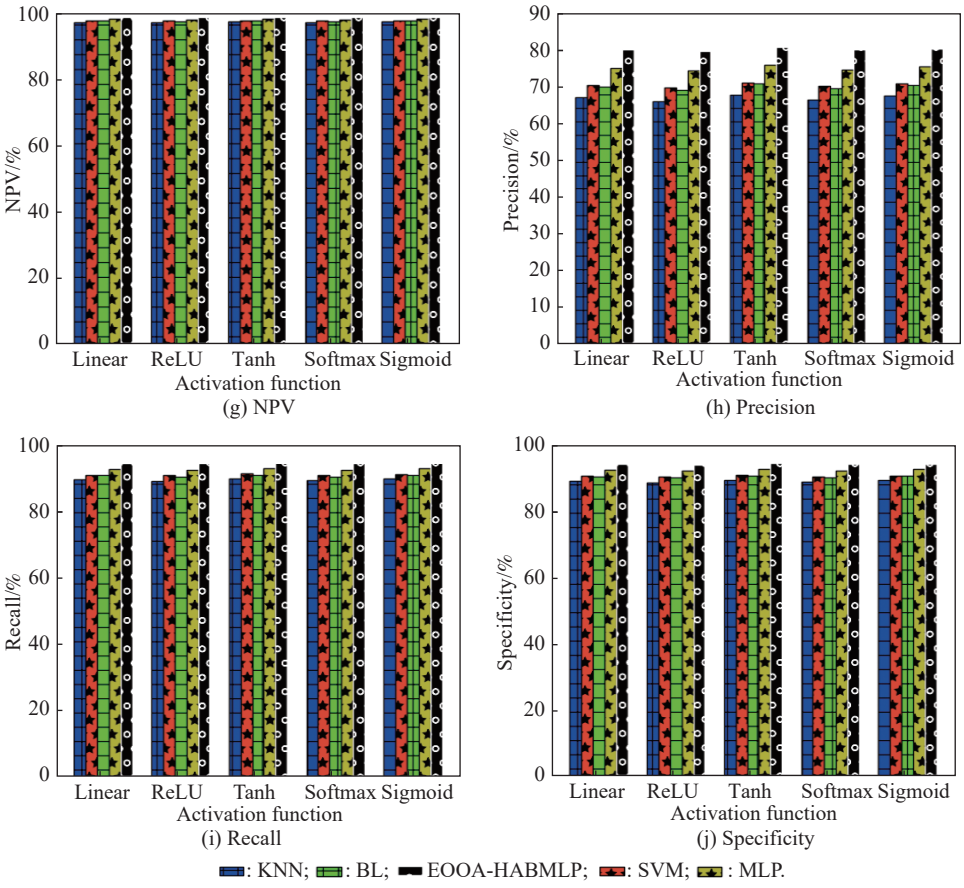
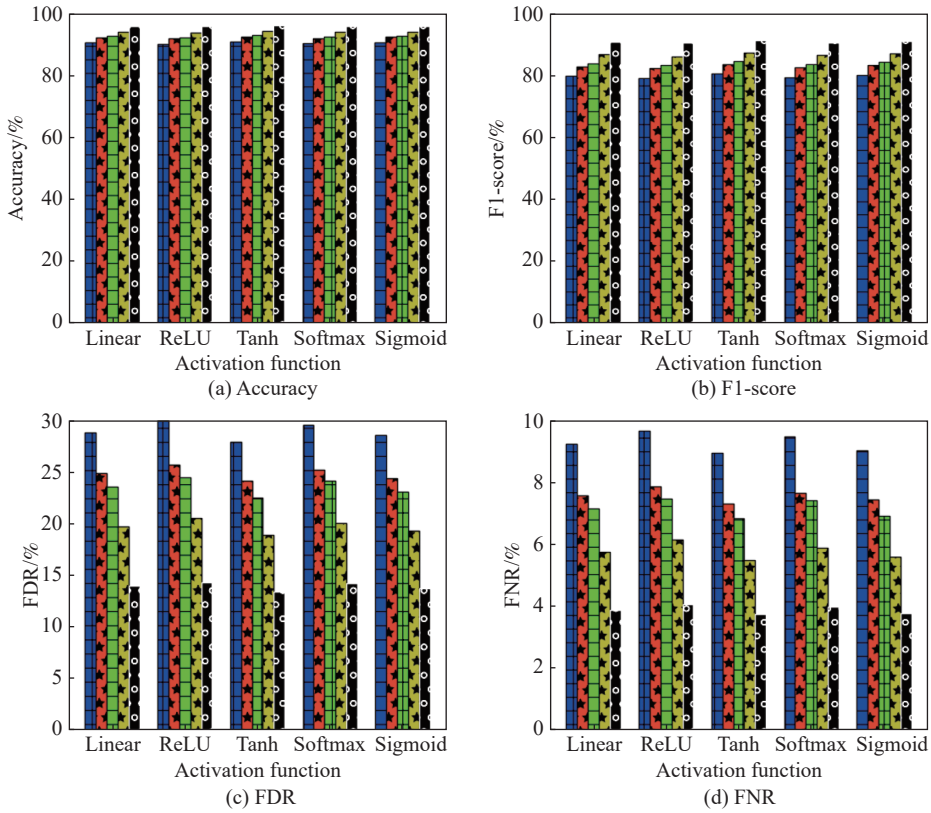


Fig. 10 Detection approach comparison of the hybrid-based GNSS spoofing detection and mitigation model for dataset 1



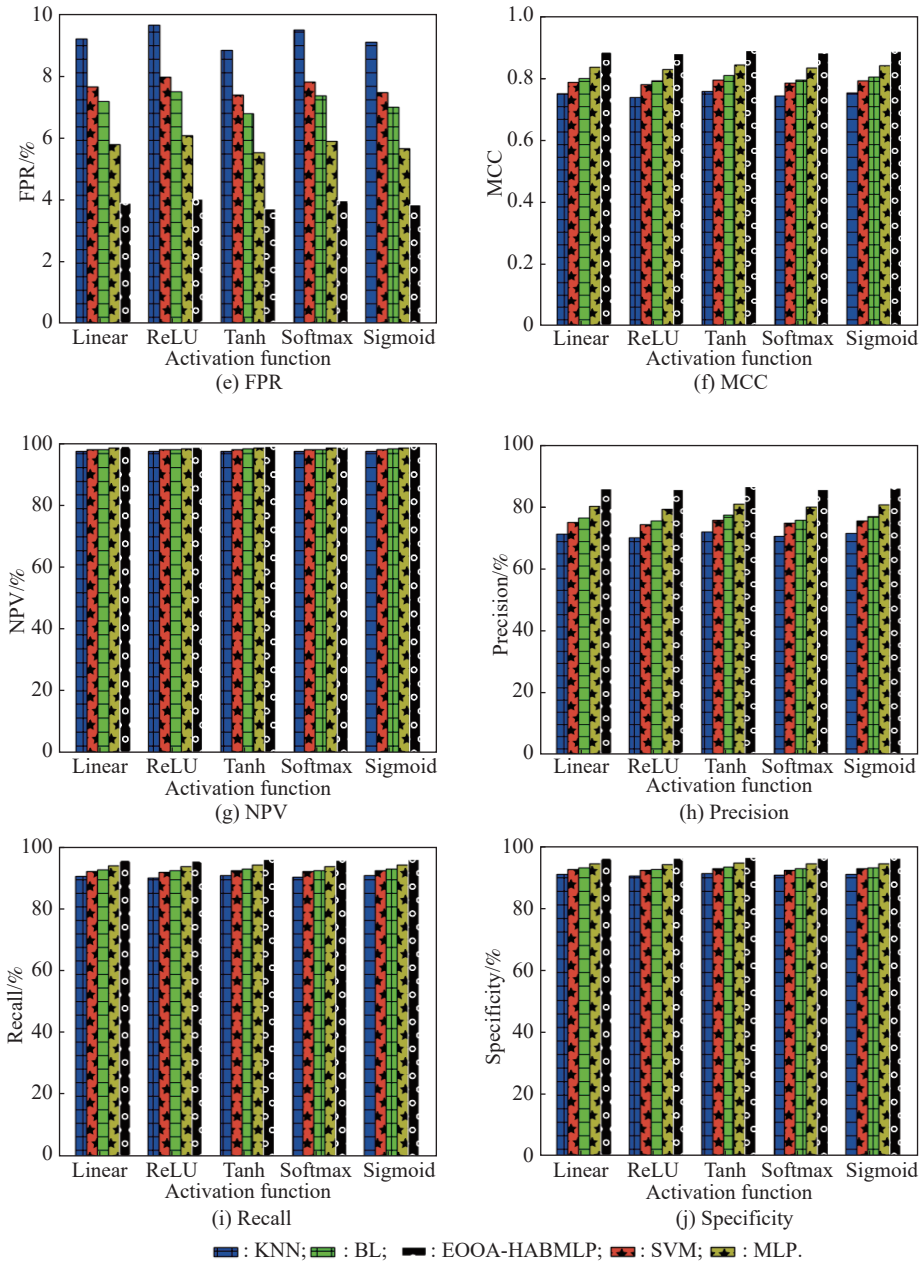


Fig. 11 Detection approach comparison of the hybrid-based GNSS spoofing detection and mitigation model for dataset 2

6.8 Statistical estimation

The statistical analysis of the designed EOOA-HABMLP-based GNSS spoofing detection and mitigation model is elucidated in Table 4. As in (18), the values should be low for the developed technique than the traditional models. In the second dataset, the best measure of the designed EOOA-HABMLP-based GNSS spoofing detection and mitigation model is 7.01%, 7.54%, 8.36%, and 8.56% boosted than the RSO-HABMLP, DMO-HABMLP, CHIO-HABMLP, OOA-HABMLP. Therefore, the performance of the EOOA-HABMLP-based GNSS spoofing recognition and mitigation method is enhanced compared to other traditional models.

Table 4 Statistical estimation of the hybrid machine learning-based GNSS spoofing detection and mitigation model

Dataset	Algorithm	RSO-HABMLP [39]	DMO-HABMLP [40]	CHIO-HABMLP [41]	OOA-HABMLP [29]	EOOA-HABMLP
Dataset 1	Mean	1.005 276	1.017 740	1.009 396	1.012 658	1.011 948
	Standard deviation	0.001 833	0.026 811	0.004 520	0.013 721	0.022 364

Continued

Dataset	Algorithm	RSO-HABMLP [39]	DMO-HABMLP [40]	CHIO-HABMLP [41]	OOA-HABMLP [29]	EOOA-HABMLP
Dataset 1	Median	1.006 534	1.003 182	1.010 223	1.007 875	1.007 321
	Best	1.002 604	1.001 809	1.003 851	1.003 888	1.000 602
	Worst	1.006 534	1.102 220	1.029 456	1.067 170	1.117 211
Dataset 2	Best	1.001 008	1.007 241	1.000 091	1.007 963	1.000 044
	Standard deviation	0.005 223	0.004 350	0.003 844	0.001 829	0.007 690
	Median	1.008 346	1.007 241	1.000 233	1.013 165	1.000 044
	Mean	1.008 852	1.009 605	1.001 348	1.011 706	1.004 360
	Worst	1.018 776	1.024 600	1.014 382	1.013 165	1.032 669

6.9 Numerical examination of the developed method

The numerical validation of the developed EOOA-HABMLP-based GNSS spoofing detection and mitigation model is listed in Table 5 and Table 6. For the first and the second datasets, the accuracy of the suggested EOOA-HABMLP-based GNSS spoofing detection and mitigation model is 94.29% and 96.27% respectively, both of these values are greater than the conventional model. Likewise, the specificity of the developed EOOA-HABMLP-based GNSS spoofing detection and mitigation method for the second dataset is 86.26%, which is greater than the KNN, SVM, BL, and MLP. Therefore, the performance of the designed EOOA-HABMLP-based GNSS spoofing detection and mitigation model is enhanced compared with other existing methods.

Table 5 Numerical investigation of the hybrid ML-based GNSS spoofing detection and mitigation model %

Datase	Term	RSO-HABMLP [31]	DMO-HABMLP [32]	CHIO-HABMLP [33]	OOA-HABMLP [26]	EOOA-HABMLP
Dataset 1	Accuracy	90.388	91.326	92.250	92.821	94.296
	Recall	90.447	91.260	92.246	92.783	94.289
	Specificity	90.373	91.342	92.251	92.831	94.297
	Precision	70.138	72.491	74.849	76.389	80.520
	FPR	9.627	8.658	7.749	7.169	5.703
	FNR	9.553	8.740	7.754	7.217	5.711
	NPV	97.425	97.664	97.942	98.093	98.508
	FDR	29.862	27.509	25.151	23.611	19.480
	F1-score	79.008	80.800	82.642	83.792	86.862
	MCC	73.89	76.12	78.43	79.85	83.67
Dataset 2	Accuracy	92.246	93.153	94.105	94.687	96.182
	Recall	92.195	93.216	94.116	94.669	96.227
	Specificity	92.259	93.138	94.103	94.691	96.171
	Precision	74.859	77.252	79.959	81.678	86.268
	FPR	7.741	6.862	5.897	5.309	3.829
	FNR	7.805	6.784	5.884	5.331	3.773
	NPV	97.929	98.212	98.461	98.612	99.029
	FDR	25.141	22.748	20.041	18.322	13.732
	F1-score	82.628	84.486	86.462	87.695	90.976
	MCC	78.404	80.726	83.422	84.470	88.776

Table 6 Technique comparison %

Dataset	Term	KNN [34]	SVM [19]	BL [29]	MLP [30]	EOOA-HABMLP
Dataset 1	Accuracy	89.283	90.678	90.540	92.541	94.296
	Recall	89.425	90.706	90.620	92.541	94.289
	Specificity	89.248	90.672	90.520	92.541	94.297
	Precision	67.525	70.853	70.500	75.619	80.520
	FPR	10.752	9.328	9.480	7.459	5.703
	FNR	10.575	9.294	9.380	7.459	5.711
	NPV	97.123	97.502	97.475	98.025	98.508
	FDR	32.475	29.147	29.500	24.381	19.480
	F1-score	76.947	79.560	79.303	83.228	86.862
	MCC	71.302	74.758	74.627	79.316	83.907
Dataset 2	Accuracy	90.945	92.555	93.046	94.375	96.182
	Recall	90.966	92.558	93.095	94.410	96.227
	Specificity	90.940	92.554	93.034	94.367	96.171
	Precision	71.510	75.654	76.964	80.731	86.268
	FPR	9.060	7.446	6.966	5.633	3.829
	FNR	9.034	7.442	6.906	5.590	3.773
	NPV	97.577	98.029	98.178	98.541	99.029
	FDR	28.490	24.346	23.036	19.269	13.732
	F1-score	80.073	83.257	84.264	87.036	90.976
	MCC	75.322	79.719	80.645	83.989	88.778

6.10 Comparative analysis of the implemented method with other state-of-the-art-techniques

Table 7 shows the comparative study of the implemented EOOA-HABMLP technique with other state-of-the-art models. In traditional techniques, timely detection is not efficient so, it affects the system performance in GNSS spoofing. However, the classical techniques are not efficient in validating larger sizes of data. Considering dataset 1, the existing SDR method shows less accuracy rate as 92.90 which can minimize overall performance in GNSS spoofing. The developed EOOA-HABMLP model shows 94.29 higher accuracy rates than the traditional models. This significant analysis in the developed model helps to manage large-size data and reduce the maximum duration of the detection process. In dataset 2, the performance validation of implemented EOOA-HABMLP is maximized by 7% SDR, 7.5% GLRT, 8.3% CNN, and 8.5% ML in terms of precision analysis. The implemented method achieves a high precision rate compared to traditional methods thus it produces better detection without any interfaces. It effectively increases the performance in the GNNS spoofing detection.

Table 7 Validation of the implemented model %

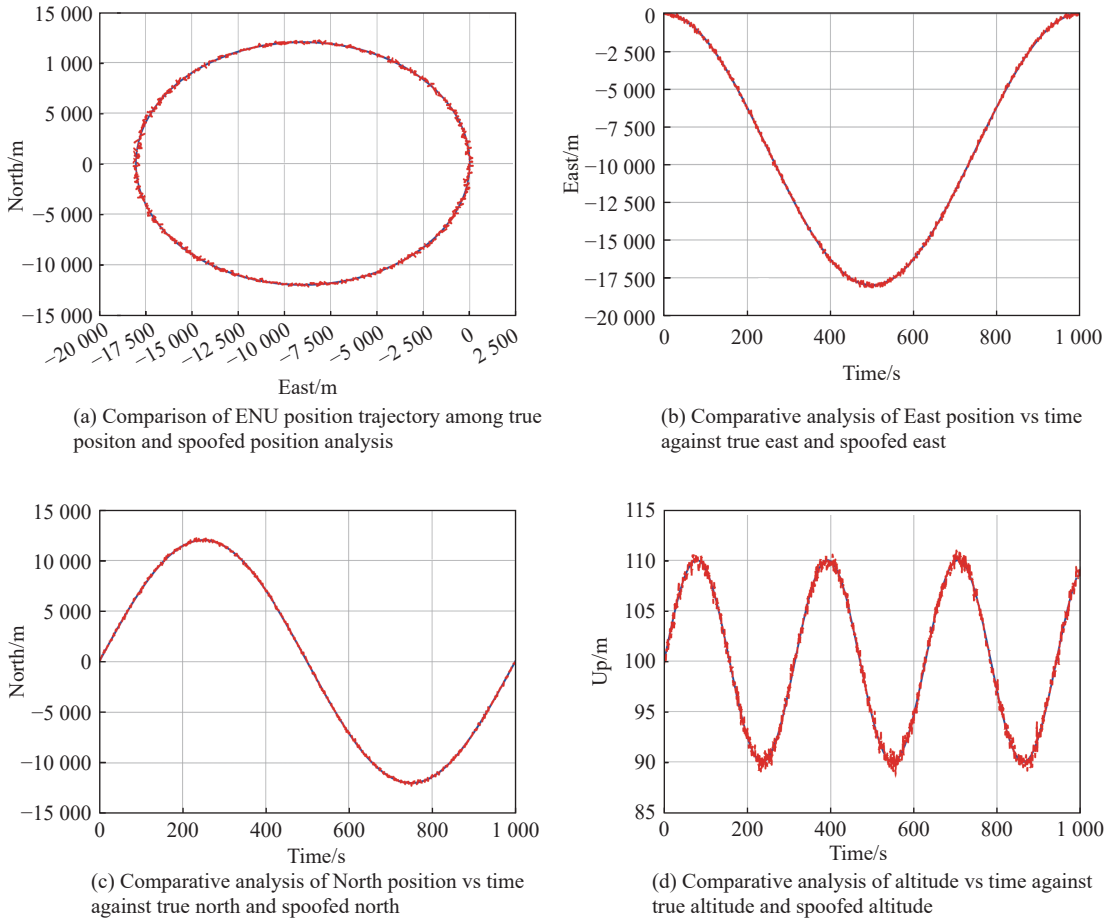
Dataset	Terms	SDR[18]	GLRT[23]	CNN[24]	ML[25]	EOOA-HABMLP
Dataset 1	Accuracy	92.901 15	93.615 55	93.787 24	94.731 92	94.295 6
	Precision	92.386 8	93.161 66	93.342 25	94.337 23	80.520 25
	Recall	92.902 62	93.602 28	93.777 2	94.738 54	94.288 68
	Specificity	92.899 78	93.627 85	93.796 56	94.725 78	94.297 33
	FPR	7.100 215	6.372 155	6.203 442	5.274 223	5.702 665
	FNR	7.097 379	6.397 716	6.222 801	5.261 464	5.711 319
	NPV	93.383 34	94.040 36	94.203 67	95.100 98	98.508 41
	FDR	7.613 203	6.838 345	6.657 753	5.662 77	19.479 75
	F1-score	92.643 99	93.381 45	93.559 22	94.537 46	86.862 24
	MCC	85.378 63	83.021 61	87.555 98	84.045 13	88.956 71

Continued

Dataset	Terms	SDR[18]	GLRT[23]	CNN[24]	ML[25]	EOOA-HABMLP
Dataset 2	Accuracy	93.233 77	93.767 72	94.536 65	94.742 69	96.182 07
	Precision	92.768 6	93.299 74	94.136 42	94.347 14	86.268 43
	Recall	93.203 48	93.782 8	94.534 23	94.751 13	96.227 07
	Specificity	93.261 87	93.753 73	94.538 89	94.734 86	96.170 82
	FPR	6.738 132	6.246 269	5.461 105	5.265 139	3.829 18
	FNR	6.796 524	6.217 203	5.465 766	5.248 87	3.772 932
	NPV	93.669 1	94.206 09	94.910 88	95.112 58	99.028 74
	FDR	7.231 399	6.700 263	5.863 583	5.652 858	13.731 57
	F1-score	92.985 53	93.540 64	94.334 91	94.548 7	90.976 03
	MCC	86.145 15	87.952 12	83.906 02	88.947 29	89.877 66

6.11 PVT analysis of the developed GNSS spoofing detection using EOOA-HABMLP

Position, velocity, and time (PVT) analysis of the developed EOOA-HABMLP method is shown in Fig. 12. PVT analysis plays a crucial role in GNSS spoofing detection performance. This analysis is used to provide valuable insights from the raw observable data. Here, the results are validated by east, north, and up (ENU) coordinate. Here, the *X*-axis is validated based on time. In the *Y*-axis, velocity, altitude, longitude, and latitude are evaluated in different ranges to show the true latitude and spoofed latitude.



(a) Comparison of ENU position trajectory among true positon and spoofed position analysis

(b) Comparative analysis of East position vs time against true east and spoofed east

(c) Comparative analysis of North position vs time against true north and spoofed north

(d) Comparative analysis of altitude vs time against true altitude and spoofed altitude

—: True north; - - -: Spoofed north.

Fig. 12 Final PVT result of the developed model

6.12 Discussion based on experimentation

In Fig. 7, shows the convergence analysis of the developed model. This analysis helps to maximize the decision-making performance and faster response in a network system. Also, it can reduce the overall processing time to provide a better solution to minimize cost function analysis. Fig. 8 represents the algorithmic examination of the proposed model. Here, several performance metrics are used to analyze the algorithmic examination process. This process helps to reduce the computational time to detect malicious activities in GNSS. Therefore, it can easily find the hackers before damaging the network to provide better security for data. Fig. 9 compares the performance of the existing and developed method detection techniques using measures like accuracy, FNR, FDR, recall, precision, specificity, NPV, F1-score, and MCC. From Fig. 9 and the second dataset, the developed EOOA-HABMLP-based GNSS spoofing detection and mitigation model accomplished the MCC value of 21.73% enhanced than the KNN, 13.04% enhanced than the SVM, 11.9% enhanced than the BL and 8.69% at tanh activation function. In FNR, the developed model produces low error rates when compared to existing approaches. This low error rate helps to improve the detection performance in the GNSS system and provides better security in the data transmission process. In Table 4, several traditional methods and the implemented model are analyzed using statistical analysis with the help of best, worst, median, mean, and standard deviation. This performance helps to handle large-size data and reduce overfitting issues. Numerical examination among traditional and developed models is shown in Table 5. Here, the precision rate is higher in the developed model to effectively provide security in the network and take less time for the detection process. This may help to improve accurate prediction while the GNSS signals are weak or obstructed. In Table 7, the comparison analysis of the implemented method and state-of-the-art method with the help of several measures is validated among two datasets. Based on this validation, the implemented method facilitates to handle errors in the system.

7. Conclusions

A hybrid machine learning-based GNSS spoofing detection and mitigation framework is developed to provide proper PVT services for civil and military applications. In addition, it has been used to provide a secure navigation process. The developed model begins with collecting the data from the online resources. This data is given to the t-SNE and PCA for retrieving the features. After that, the features obtained from the t-SNE and PCA are given to the HABMLP made up of BL and MLP. This structure processed with the extracted feature for getting the predicted outcome. Here, the EOOA is adopted to tune the parameters in the HABMLP and enhance the performance in the GNSS spoofing detection and mitigation process. The result from the BL and MLP is averaged to get the final detected outcome. The developed model used a very small number of hardware requirements for detecting the GNSS spoofing. The detected GNSS spoofing is also mitigated by the same HABMLP. The developed model is applicable in navigation, traffic control, and airborne traffic control systems for providing PVT services. The probability distribution of the Bayes learning method sometimes affects the accuracy of the detection, which has solved in upcoming work with the support of advanced machine learning techniques. In future work, the implementation of real-time data will be needed to show better performance enhancement in GNSS spoofing detection and mitigation framework. Complex multipath conditions will be needed for developing different spoofing cases in detection performance. Further, likelihood ratio test (LRT)-based framework will be focused on future work for detecting live spoof in satellites. Additionally, the implementation of 3D mapping technique in urban environment will be required for rapidly detecting the advanced spoofing in GNSS system.

References

[1] CYNTHIA J, RATHI S. A novel EKF-integrated attention-enhanced CNN-GRU framework for precise GPS spoofing detection. Signal, Image and Video Processing, 2025, 19(6): 491–502.

[2] BADAR A U R, MAHMOOD D, IQBAL A, et al. DeepSpoofNet: a framework for securing UAVs against GPS spoofing attacks. PeerJ Computer Science, 2025, 11: e2714.

[3] LIU C X, REN B B, XIE Y C, et al. Deep learning-based GNSS composite jamming detection and recognition technology. Frontiers in Signal Processing, 2025, 5: 1567926.

[4] ABDULLAYEVA F, VALIKHANLI O. Multimodal deep neural network for UAV GPS jamming attack detection. Cyber Security and Applications, 2025, 3: 100094.

[5] ZHUANG X B, NIU B, LIN Z J, et al. A multiparameter spoofing detection method based on parallel CNN-Transformer neural network with gating mechanism. Journal of Electronics & Information Technology, 2025, 47(3): 567–578.

[6] BALDINI G, BONAVITACOLA F. A machine learning evaluation of the impact of bit-depth for the detection and classification of wireless interferences in Global Navigation Satellite Systems. Electronics, 2025, 14(6): 1147.

[7] KWON K C, SHIM D S. Performance analysis of direct GNSS spoofing detection with accelerometers for constant velocity. International Journal of Control, Automation and Systems, 2022, 20(8): 2749–2758.

[8] HAO Y, SHI C, XU A, et al. Revealing methods of GNSS spoofing mitigation through analyzing the spoofing impacts

on adaptively robust estimation-based RTK/INS tightly coupled integration. IEEE Sensors Journal, 2023, 23(20): 25165–25178.

[9] LEMIESZEWSKI Ł. Transport safety: GNSS spoofing detection using the single-antenna receiver and the speedometer of a vehicle. Procedia Computer Science, 2022, 207: 3181–3188.

[10] ALMADHOR A, BAILI J, ALSUBAI S, et al. CTDNN-Spoof: compact tiny deep learning architecture for detection and multi-label classification of GPS spoofing attacks in small UAVs. Scientific Reports, 2025, 15: 6656.

[11] CHEN F Q, LIU Z, HUANG L, et al. GNSS interference mitigation method based on deep learning. Frontiers in Physics, 2025, 13: 1535906.

[12] WANG Y W, KOU Y H, ZHAO Y, et al. Detection of synchronous spoofing on a GNSS receiver using weighed double ratio metrics. GPS Solutions, 2022, 26(3): 91.

[13] FENG F, CHEN Z K, CHEN L J, et al. Rapid detection of GNSS time synchronization attacks via the enhanced code and carrier Doppler consistency test. GPS Solutions, 2024, 28(3): 38.

[14] CHEN Z Y, LI H, WEI Y M, et al. GNSS antispoofing method using the intersection angle between two directions of arrival (IA-DOA) for multiantenna receivers. GPS Solutions, 2023, 27(1): 11.

[15] SEO S H, JEE G I, LEE B H. Spoofing signal generation based on manipulation of code delay and Doppler frequency of authentic GPS signal. International Journal of Control, Automation and Systems, 2021, 19(4): 1026–1040.

[16] AL-SABBAGH A, EL-BOKHARY A, EL-KOUSSA S, et al. Enhancing UAV security against GPS spoofing attacks through a genetic algorithm-driven deep learning framework. Information, 2025, 16(2): 115.

[17] CHEN Y K, ZHAN X Q. GNSS vulnerability reliable assessment and its substitution with visual-inertial navigation. Aerospace Systems, 2021, 4(3): 179–189.

[18] MENG Q, HSU L T, XU B, et al. A GPS spoofing generator using an open sourced vector tracking-based receiver. Sensors (Special Issue on Interference, Robustness and Complementary Solutions for GNSS-Based Navigation for Aerial Vehicles), 2019, 19(18): 3993.

[19] SEMANJSKI S, MULS A, SEMANJSKI I, et al. Use and validation of supervised machine learning approach for detection of GNSS signal spoofing. Proc. of the International Conference on Localization and GNSS (ICL-GNSS), 2019: 1–6. DOI: 10.1109/ICL-GNSS.2019.8752775.

[20] SHANG F Y, SUN B P, LIU L D, et al. Mitigation of GNSS time synchronization attacks in a multicorrelator receiver. IEEE Access, 2022, 10: 70383–70393.

[21] SINGH S, SINGH J, SINGH S S. Mitigating spoofed GNSS trajectories through nature inspired algorithm. GeoInformatica, 2021, 25(3): 581–600.

[22] SCHMIDT E, GATSIS N, AKOPIAN D. A GPS spoofing detection and classification correlator-based technique using the LASSO. IEEE Trans. on Aerospace and Electronic Systems, 2020, 56(6): 4224–4237.

[23] PARDHASARADHI B, SRINATH G, VANDANA S G, et al. GNSS spoofing detection and mitigation in multireceiver configuration via tracklets and spoofer localization. IEEE Access, 2022, 10: 42014–42028.

[24] BLAIS A, COUELLAN N, MUNIN E. A novel image representation of GNSS correlation for deep learning multipath detection. Array, 2022, 14: 100167.

[25] NAYFEH M, LI Y, AL SHAMAILEH K, et al. Machine learning modeling of GPS features with applications to UAV location spoofing detection and classification. Computers & Security, 2023, 126: 103085.

[26] TAKIGUCHI MEDINA E, LOHAN E S. GNSS spoofing modeling and consistency-check-based spoofing mitigation with Android raw data. Electronics, 2025, 14(5): 898.

[27] LI J, WU H, GAO J, et al. Performance testing and analysis of a new GNSS spoofing detection method in different spoofing scenarios. IEEE Access, 2025, 13: 54779–54793.

[28] TRÝB J, HOSPODKA J. GNSS interference and security: Impacts on critical infrastructure and mitigation strategies. Procedia Computer Science, 2025, 253: 2635–2644.

[29] DEHGANI M, TROJOVSKÝ P. Osprey optimization algorithm: a new bio-inspired metaheuristic algorithm for solving engineering optimization problems. Frontiers in Mechanical Engineering, 2023, 8: 1126450.

[30] WANG S Q, LIU J, CAI B G, et al. Anti-spoofing performance analysis of typical GNSS-based railway train positioning schemes. High-speed Railway, 2025, 3(1): 37–43.

[31] VENTURINO A, D'AFFLISIO E, FORTI N, et al. Adaptive resilience navigation filter for detecting and mitigating multi-spoofing attacks in range-based localization systems using antenna arrays. IEEE Trans. on Aerospace and Electronic Systems, 2025, 61(3): 6856–6872.

[32] HOSSAIN M M, HOSSAIN M A, MIAH A S M, et al. Stochastic neighbor embedding feature-based hyperspectral image classification using 3D convolutional neural network. Electronics, 2023, 12(9): 2082.

[33] SOPHIAN A, TIAN G Y, TAYLOR D, et al. A feature extraction technique based on principal component analysis for pulsed Eddy current NDT. NDT& E International, 2003, 36(1): 37–41.

[34] ÁLVAREZ-MOLINA X, SECO-GRANADOS G, SOLÉ-GASET M, et al. Performance analysis of spoofing and interference detection techniques for Satellite-Based Augmentation System and Global Navigation Satellite System reference receivers. Engineering Proceedings, 2025, 88(1): 38.

[35] GOPNIK A, TENENBAUM J B. Blackwell Publishing Ltd Bayesian special section: introduction Bayesian networks, Bayesian learning, and cognitive development. Developmental Science, 2007, 10(3): 281–287.

[36] TARIQ U, TARIQ B. Signal characteristic analysis and anomaly detection for GPS spoofing mitigation. Ubiquitous Technology Journal, 2025, 1(1): 10–22.

[37] VASOU JOUYBARI M, ATAIE E, BASTAM M. An MLP-based deep learning approach for detecting DDoS attacks. Tabriz Journal of Electrical Engineering, 2022, 52(3): 195–204.

[38] ZHANG S, SUN C, XU Y, et al. Principal component analysis-based optimal feature design for GNSS spoofing detection. IEEE Communications Letters, 2025, 1: 1.

[39] ZEBIRI I, ZEGHIDA D, REDJIMI M. Rat swarm optimizer for data clustering. Jordanian Journal of Computers and Information Technology, 2022, 8(3): 297–307.

[40] AGUSHAKA J O, EZUGWU A E, ABUALIGAH L. Dwarf mongoose optimization algorithm. Computer Methods in Applied Mechanics and Engineering, 2022, 391: 114570.

[41] AL-BETAR M A, ALYASSERI Z A A, AWADALLAH M A, et al. Coronavirus herd immunity optimizer. Neural Computing and Applications, 2021, 33(10): 5011–5042.

[42] MA X M, SUN T H, GAO M G. A reinforcement learning-enhanced spoofing algorithm for UAV with GPS/INS-integrated navigation. IEEE Trans. on Aerospace and Electronic Systems, 2025, 61(4): 8659–8673.
[43] LI J, CHEN Z, YUAN X, et al. A real-time GNSS time spoofing detection framework based on feature processing. GPS Solutions, 2025, 29(1): 45.
[44] SPANGHERO M, GEIB F, PANIER R, et al. GNSS jammer localization and identification with airborne commercial GNSS receivers. IEEE Trans. on Information Forensics and Security, 2025, 20: 3550–3565.
[45] TOHIDI S, MOSAVI M R. Effective detection of GNSS spoofing attack using a multi-layer perceptron neural network classifier trained by PSO. Proc. of the 25th International Computer Conference, 2020. DOI: 10.1109/CSICC49403.2020.9050078.