IUST
Iran University of Science and Technology

Iranian Journal of Electrical and Electronic Engineering

Journal Homepage: ijeee.iust.ac.ir

A Deep Learning Based Code Loop Discriminator for GPS Spoofing Mitigation

S. Tohidi*, M. R. Mosavi*(C.A.)

Abstract: A vital part of people's daily life is the position, navigation, and time service provided by the Global Positioning System (GPS), which is always accessible globally. Consequently, the security of the GPS receivers is crucial. Occasionally, intentional and unintentional interferences cause GPS location issues. Spoofing attack is the most severe interference to the GPS receivers, which results in positional mistakes. This paper's goal is to defend against the carry-off spoofing attacks. In a carry-off spoofing attempt, the spoofer transmits signals whose code phase and carrier frequency parameters are strikingly close to the actual signal in order to change the correlation values generated in the tracking stage. Discriminator output values alter as correlation values change. As a result, the Pseudo Random Noise (PRN) code generator unit creates a local replica, which forces the tracking loop to follow the fake signal instead of the real one. It is proposed in this paper that when spoofing attacks occur, discriminator output values be generated independently of correlation values. Specifically, when a spoofing signal is detected, the conventional discriminator is replaced by a Non-linear Autoregressive Exogenous Neural Network (NARX NN)-based predictor. This strategy protects the tracking loop from the effects of the spoofing signal. The efficiency of the provided strategy was evaluated using three spoofing data sets. The results of the suggested mitigation method, based on NARAX NN, show that it mitigates spoofing attacks by an average of 95.82%.

Keywords: GPS, DLL, Spoofing Attack, Non-linear Autoregressive Exogenous Neural Network.

1 Introduction

THE widely used Global Positioning System (GPS) can provide continuous global position, navigation, and time service. It is proven that civilian GPS signals are vulnerable to spoofing attacks because of their low received power and open structure [1,2]. The objective of spoofing is to force the victim receiver to yield a misleading position solution.

Since the GPS satellites are in continuous motion, the receiver must ensure that the signals emitting from the satellites are continuously tracked and monitored. So, it is required in a GPS receiver to maintain continuous synchronization with visible satellite signals for range measurements, extraction of ephemeris data, and position, navigation, and time estimation. In conventional GPS receivers, tracking loops are employed for joint fine-tuning of the incoming signal to the residual Doppler carrier frequency and phase offsets and spreading code alignment. When the receiver is tracking an authentic signal, the code phase and the carrier frequency of the spoofing signal must match those of the authentic signal; otherwise, even very powerful spoofing signals cannot take over the receiver [3].

The critical feature for a spoofing attack is to be able to gradually drag off the tracking points without unlocking the victim receiver's code and carrier loop. [4]. Su et al. [5] developed a novel spoofing mitigation algorithm leveraging a single 5G base station (BS). In their proposed approach, the concept of anomaly detection

Iranian Journal of Electrical & Electronic Engineering, 2026.
Paper first received 15 Jan. 2025 and accepted 24 Jun. 2025.
* The authors are with the School of Electrical Engineering, Iran University of Science and Technology (IUST), Narmak, Tehran 16846-13114, Iran.
E-mails: s_tohidi@elec.iust.ac.ir and m_mosavi@iust.ac.ir.
Corresponding Author: M. R. Mosavi

was extended to the GNSS-5G fusion positioning system to identify spoofing attacks. Subsequently, a true position estimation algorithm was introduced. Initially, the authors established the fusion EKF (Extended Kalman Filter) output model and provided its mathematical derivation. A coarse position estimate was obtained by combining the GNSS-spoofed position and the GNSS-5G fusion positioning results. Fine position estimation was then carried out using an additional EKF with inputs from the coarse estimates and secure 5G measurements, thereby enhancing the accuracy of the true position estimate.

In another study [6], the multipath estimating delay lock loop (MEDLL), originally designed for multipath mitigation, was employed in conjunction with the Inertial Navigation System (INS) to counter spoofing attacks. The approach first utilized a bank of correlators to estimate both the spoofed and authentic signals. A new spoofing validation and mitigation structure was then proposed, based on the tightly coupled INS/GNSS integrated system. Finally, an INS-aided reacquisition and spoofing suppression method was derived.

In [7], the authors proposed two cascaded estimation algorithms for concurrent GNSS spoofing detection and localization in a multi-UAV scenario, aiming to achieve robust navigation in environments subject to GNSS spoofing attacks.

The authors in [8] leveraged the fact that, under most attack modes, both authentic and spoofed signals are received by the victim. Once an attack is detected using conventional spoofing detection methods, the receiver scans for secondary peaks in the vicinity of each satellite signal’s correlation peak. Meanwhile, navigation continues in dead reckoning mode, relying on other sensors and the user’s dynamics model. A decision regarding which signals to trust is then made in the position domain. Once enough secondary peaks are detected, multiple navigation solutions are generated by combining the main and secondary peaks.

In [9], the authors proposed a GNSS spoofing suppression method based on spoofing correlation peak cancellation (SCPC). This method estimates the spoofing signal from the baseband sampling sequence and generates a reverse cancellation sequence to suppress the GNSS spoofing attack. Based on this technique, a receiver scheme with an SCPC function was proposed by adding a suppression module to the general GNSS receiver model.

Numerous detection and mitigation methods have been proposed to enhance the security of GPS receivers against spoofing attacks. These studies can be categorized into five distinct groups.

Cryptographic signal authentication methods rely on unpredictable information carried by the encrypted GNSS signal to ensure its authenticity. The problem with this method's efficiency is that no open civil GNSS signal yet incorporates cryptographic modulation [10-14].

TOA anomaly detection methods depend on a delay between the spoofing data bit boundaries and those of the authentic ones [15]. These methods are not effective when the spoofer has the ability to predict GPS bits.

The premise of spatial processing techniques is that since spoof signals are emitted from a single antenna, they all have the same direction, including numerous Pseudo Random Noise (PRN) signals [16-18]. On the other hand, authentic signals are received from different directions because their transmission sources are different satellites. According to [19,20] studies, spatial processing methods fall into three subcategories, namely antenna array processing [21], moving receiver and network/cloud-based [22,23].

Methods based on the signal power anomaly detection consider any sudden change in strength as being related to the presence of interference. The authors of [24] detect the spoofer by monitoring the rate of power changes in the signal. The authors of [25] created a test procedure for determining how civil GPS receivers respond to spoofing attacks. They examined the spoofer signal's power advantage over authentic signals needed for effective receiver capture properties. Results of the test process show that just around 1.1 times as much spoofing signal power as authentic signal power is needed to consistently capture a target receiver. The authors of [26] detected the presence of high-power spoofing signals using abnormally high C/N_0 values. Because GPS satellites are 20,000 kilometers away, any position change of a receiver near the earth's surface should not significantly alter signal power. However, because received power is highly dependent on the environment, such as antenna attitude and multi-path, this method is only applicable to static observations.

The interaction of authentic signals with spoofing results in distortion of the correlation function's shape. Correlation monitoring methods rely on scrutinizing the outputs of correlators. The authors of [27] used Signal Quality Monitoring (SQM) tests, widely used to detect distortion on the correlation function caused by multi-path, to detect GPS spoofing attacks. The study cited in [28] investigated the effectiveness of the ratio metric in detecting spoofing attacks. [29] proposed a method based on distortion monitoring in the complex correlation domain to detect spoofing attacks. [30] increased the number of correlators and presented a spoofing detector based on the SQM technique. [31] illustrated that combining correlation monitoring metrics

and methods based on monitoring the received signal strength yields more efficient results. A two-dimensional SQM detector in the frequency domain was suggested by [32]. The study cited in [2] employed symmetric difference, which is a common distortion measurement, and the power of the received signal for interference detection. [33] presented a power-distortion detector, which utilized a maximum-likelihood multi-path estimator and employed the magnitude of its normalized post-fit residuals to monitor distortion in the correlation function. They demonstrated that interference detection performance could be improved significantly compared to approaches that employ symmetric difference as a distortion metric.

Contributions of This Paper: This paper addresses carry-off spoofing attacks and is based on advanced signal-processing techniques in the GPS receiver's tracking stage with a mitigation extent. The proposed method falls into the correlation monitoring-based methods. Practical short-term spoofing detection and mitigation techniques are low-cost, do not require additional hardware, can be implemented through a software or firmware update, do not require changes in GPS signals in space, and are receiver independent. These are a few benefits of correlation monitoring-based techniques.

GPS signal processing commonly uses a correlation-based synchronization of locally generated replicas of expected signal patterns with received signals. The correlations of the received signal with locally replica fragments generated with various time delays manufacture a correlation profile. Significantly, an ideal correlation profile of a GPS C/A signal resembles a triangle function. The problem we face in the carry-off spoofing attack is the distortion in the correlation profile due to the counterfeit signal, which researchers have introduced different criteria to detect. In all those methods, an attempt is made to introduce a criterion that can detect spoofing by examining the correlation profile. However, developing the tracking loop to make the GPS receiver robust against the detected spoof is an issue that has rarely been addressed. The distortions brought on by the spoofer can affect the Delay-Locked Loop (DLL), which is the largest issue with spoofing mitigation in the GPS receivers tracking stage. In the current study, we use artificial intelligence techniques to try and stop this adverse effect.

In a carry-off spoof, the attacker attempts to align the spoofing signal with the real signal. The aligned spoofing signal has a considerable impact on the tracking loop's correlator output values and variations in the output values of the correlations affect the discriminator's output. The local signal will then be modified in the following round of tracking by the PRN code generator unit that use the discrimination output. Through this process, the tracking loop finally tracks the fake signal instead of the real one. Thus, discrimination is a key component of the tracking loop since it chooses the signal to be tracked.

In the current study, it is recommended that the discriminator be designed using a Neural Network (NN). In the face of a spoofing attack, a NN-based discriminator can examine the natural trend of GPS data. In particular, a Non-linear Autoregressive Exogenous Neural Network (NARX NN) is used. The NN's dependence on training data, which consists of signal features, is an advantage that we seek.

The following section describes the signal model. Methodology and configuration of the NARX NN is described in detail next. Then, a discussion of the results is stated. Finally, a conclusion is provided.

2 Signal Model

GPS satellites transmit navigation data and codes in two frequency bands: L1 and L2. Only the L1 signal, which is available for civilian use, is examined here. In general, the GPS receiver's model of the signal received from satellite number i is given by Eq. (1):

$$x(t) = S_{Ii}(t) + n(t) + I(t) = \sqrt{2P_t}\, d_i(t) c_i(t) \cos(2\pi f_{li} t + \theta) + n(t) + I(t) \quad (1)$$

where $S_{LIi}(t)$ represents the satellite signal in L1 frequency band, P_t denotes the power of the carrier signal, $d_i(t)$ symbolizes navigation information, $C_i(t)$ represents the pseudo-random sequence (C/A code), f_{L1} indicate the frequency of the L1 carrier (1575.42 MHz), n(t) denotes noise, and $I(t)$ shows the source of interference in GPS. The structure of spoofing signal is defined according to Eq. (2):

$$\mathrm{I(t)} = \sqrt{2\,\mathrm{P_s}}\ \mathrm{c_i(t+t)} \cos(2\,\mathrm{pf_{L1}t+j}) \quad (2)$$

where P_s denotes the power of the spoofing signal

Traditional GPS receivers synchronize the locally produced signal with the received signal using two tracking loops, a Frequency Lock Loops (FLLs) or Phase Lock Loops (PLLs) and a DLL. The idea behind the DLL is to correlate three replicas of the code, the late, prompt, and early with the input signal. The output of these integrations is a term indicating how much the code in the incoming signal correlates with the specific code replica. The code phase error on the local code replica is find by using a code discriminator block. Fig. 1 shows the basic block diagram of code tracking loop. where y(n) R and u(n) R represent the model's output and input at discrete time step n, respectively, and dy ≥ 1

and du ≥ 1 the output- and input-memory orders, respectively. The function f(.) represents the NN's non-linear function. It can be seen that the output data can be used as input in the feedback function to improve the network's accuracy via open loop or closed loop training.

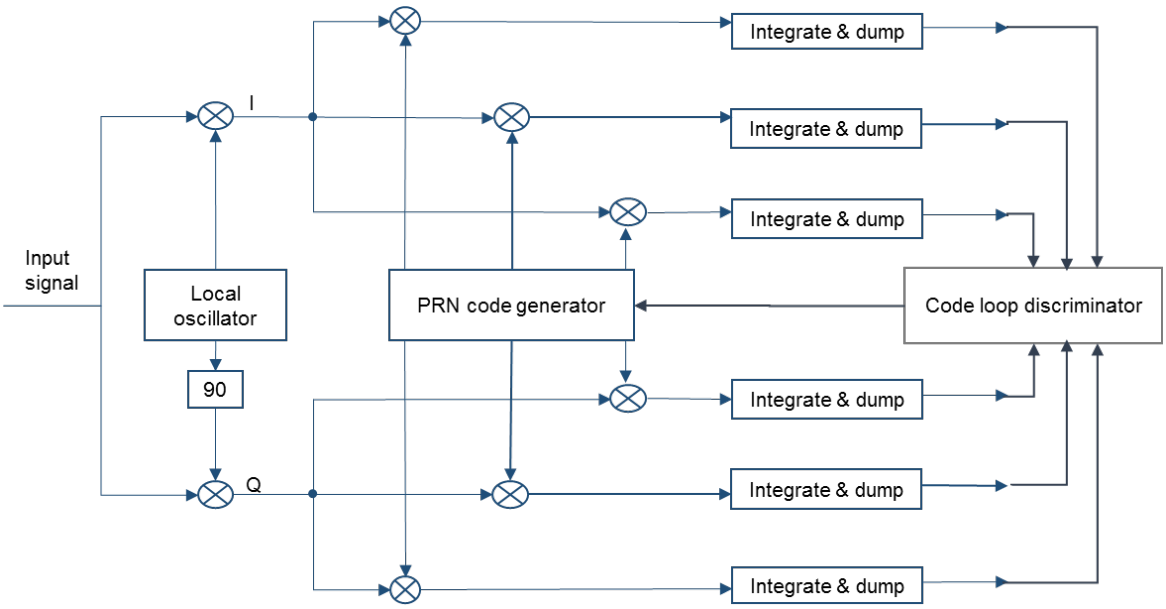

Fig 1. A block diagram of a code tracking loop.

The discriminator output, which is the code phase error, is used as a control signal for the PRN code generator. The upper half of Fig. 1 is referred to as the in-phase (I) arm, while the lower half is referred to as the quadrature (Q) arm. The signal Q is multiplied by three code replicas before being integrated and dumped. I_L, I_P, I_E, Q_L, Q_P, and Q_E are the final outputs of six correlators. The outputs of the six correlators are sent to the code loop discriminator once they have been obtained. The code loop discriminator is based on an algorithm, which is explained in more detail below [34].

Coherent discriminator: The most basic of all discriminators is the coherent discriminator. The quadrature arm is not required for this method. This method is only applicable when the local carrier signal and the incoming carrier signal are perfectly aligned.

$$D = I_E - I_I \tag{3}$$

Early minus late power (non-coherent discriminator): Within nominal chipping rates of C/A code, the response of this type of discriminator is nearly identical to that of coherent discriminator.

$$D = (I_e^2 + Q_E^2) - (I_l^2 + Q_L^2) \tag{4}$$

Dot product (non-coherent discriminator): This is the only discriminator that uses all six correlator outputs.

$$D = I_P(I_E - I_L) + Q_P(Q_E - Q_L) \tag{5}$$

Normalized early minus late power (non-coherent discriminator): This method outperforms the others. Because it invokes both the in phase and quadrature arms, the response of this discriminator is independent of the performance of the PLL. Furthermore, this enables the DLL to keep track of the signal even when the chip error exceeds the nominal chipping rate of C/A code.

$$D = \frac{(I_e^2 + Q_E^2) - (I_l^2 + Q_L^2)}{(I_e^2 + Q_E^2) + (I_l^2 + Q_L^2)} \tag{6}$$

In this paper, we want to introduce new code discriminator based on NN that can mitigate the spoofing attack. The aim of this paper is introducing a new code discriminator of the GPS receiver based on NN to mitigate the spoofing attack.

3 NARX NN for Spoof Mitigation: Basics and Mechanism

In order to mitigate carry-off spoofing attacks, we provide NARX NN to forecast discriminator output under spoofing attack circumstances. Fig. 2 shows a block diagram of the research methodology. Referring to Fig. 2, the digitized received IF signal is being mixed with the replica carrier signals to produce I and Q sampled data. The I and Q signals have the desired phase relationships with respect to the detected carrier of the received signal at the mixers' outputs. The replica carrier signal is synthesized by the carrier NCO. The Q and I signals are then correlated with prompt, early, and late replica codes that are synthesized by the PRN code

generator. Afterward, correlation results are accumulated. And accumulated and dump module output is fed to discriminator units. In closed loop operation, the PRN code generator which is used for precision code generation is controlled by the code discriminator. Also, the correlator outputs are provided to the detector.

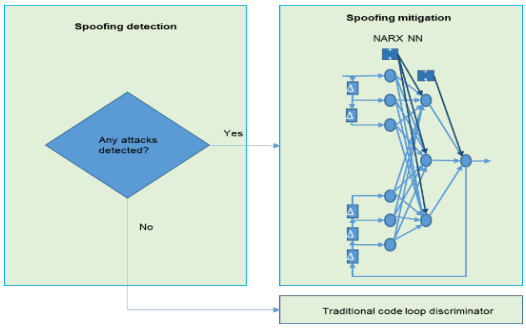

Fig 2. General schematic design of the suggested model to predict the discriminator outputs.

In present study, the NARX NN-based predictor is employed in the discriminator unit so that it can modify the output value of the code discriminator once the spoofing detection unit raises the alarm. It should be noted that in the detection unit, we used the fuzzy classifier based on time–frequency analysis method [35].

The NARX NN technique is an essential category of non-linear Dynamic Recurrent Neural Network (DRNN) comprising linked nodes inspired by simplifying the human neural system. Dynamic networks are capable of forecasting the pattern of non-linear functions and modeling arbitrary non-linear dynamical systems, and it is especially helpful in time series representing [36,37].

In simpler terms, a NARX neural network is a type of recurrent neural network specifically designed for time series modeling, where the present output is influenced by previous values of both the inputs and outputs. It is particularly well-suited for dynamic system modeling and time series forecasting. Key features of a NARX NN include:
(1) **Effective dynamic system modeling** – It captures temporal dependencies through output feedback, making it ideal for applications such as control and prediction. (2) **Dual operation modes** – The network can function in either open-loop or closed-loop configurations. (3) **Nonlinear and flexible** – Leveraging neural networks allows it to model complex, nonlinear relationships, offering greater expressiveness than traditional linear autoregressive models. (4) **Improved stability and interpretability** – The use of delayed feedback and external inputs makes the model more structured and interpretable compared to generic recurrent neural networks. The architecture of a NARX neural network is illustrated in Fig. 3.

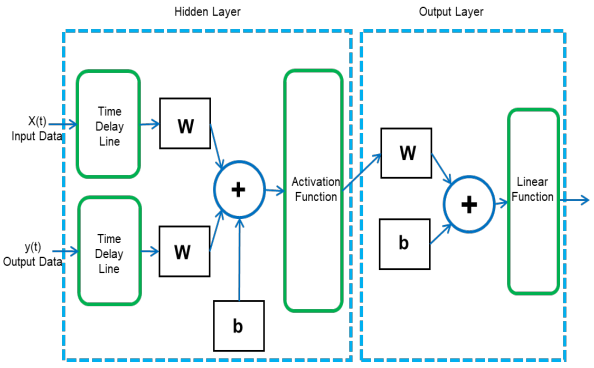

Fig 3. The block diagram of a NARX NN.

The feedforward NN model's input signal propagates forward through the structure, which can have one or more hidden layers. However, in a NARX NN and, more broadly, in DRNN architecture, information propagates forward and backward, connecting neurons in previous or the same layers. This structure compares the current level of an incoming time series to earlier values of the same sequence and the previous and current values of exogenous series. In a typical NARX regression network, the input layer, hidden layer, output layer, and output and input delay are all present, with feedback connections enclosing several layers of the network.

Some important characteristics of NARX networks have been reported when compared to other NN types: (1) these networks generalize better than other networks; (2) NARX networks converge much faster; (3) learning is more effective in these networks; and (4) NARX networks are often much better at discovering long time-dependences than conventional DRNNs [38,39].

A NARX NN can be represented mathematically as follows:

$$y(n+1) = f\left(y(n), y(n-1), \ldots, y(n-d_y), u(n), \ldots, u(n-d_u)\right) \quad (7)$$

where y(n) R and u(n) R represent the model's output and input at discrete time step n, respectively, and $d_y \geq 1$ and du ≥ 1 the output- and input-memory orders, respectively. The function f(.) represents the NN's non-linear function. It can be seen that the output data can be used as input in the feedback function to improve the network's accuracy via open loop or closed loop training.

4 Proposed NARX NN Structure

The ultimate goal of a carry-off spoofing attack is to modify the correlator's output in order to capture the tracking loop; thus, a NARX NN can be of great assistance in estimating the authentic trend of the discriminator's output and protecting the receiver from the disastrous consequences of a spoofing attack.

In order to develop the NARX model to achieve the desired results, it is necessary to select the network

features appropriately, such as the input and output delays, the number of neurons, and the training algorithm.

Generally, the hidden layer's size is highly dependent on the number of input nodes. There are several ad-hoc approaches for selecting the appropriate number of hidden neurons. The trial-and-error procedure is one of the popular methods for making optimal decisions [40] that here we use it. We perform a grid search for preferring the optimal number of the hidden layer neurons and delay components.

The decision is directed by considering the trade-off between the validation error of the training process and computational complexity. The Levenberg Marquardt Back-Propagation (BP) algorithm performs parameter optimization by searching the hyperparameter space. Finally, we determined the number of input delay components to be 18, the number of output delay components to be 2 and the number of hidden layer neurons to be 19.

4.1 NARX NN Training

There are two general approaches to NARX NN training. The first is the dynamic BP algorithm, which requires computing the gradients for learning purposes. Dynamic network error surfaces can be more difficult to compute than static network error surfaces. Also, the gradients must be computed using this method, which takes more time and is more computationally intensive than static BP algorithm. Furthermore, training is more likely to become trapped in local minima. The second algorithm is the static BP algorithm based on a series-parallel configuration. Because the actual output is available during the network's training, this method considers it rather than feeding back the estimated production of the NARX network. This configuration has two benefits. The first is that the resulting network has a pure feedforward architecture and can be trained using static BP algorithm. The second benefit is that the feedforward network's input is more accurate. As a result, we went with the second option.

Fig. 4 depicts the NARX NN architecture. The parameters of the network are as follows:

$$X(n) = \left[u(n), u(n-1), ..., u(n-d_u), y(n-1), ...y(n-d_y)\right]^T \quad (8)$$

$$W^I(n) = \begin{bmatrix} w_{11}(n) \cdots w_{1k}(n) \\ \vdots \quad \ddots \quad \vdots \\ w_{l1}(n) \cdots w_{lk}(n) \end{bmatrix} \quad (9)$$

$$\Phi^I(n) = \left[\varphi_1^I(n), \varphi_2^I(n), \cdots, \varphi_k^I(n)\right]^T \quad (10)$$

$$\Phi^O(n) = \left[\varphi_1^o(n), \varphi_2^o(n), \cdots, \varphi_k^o(n)\right]^T \quad (11)$$

$$W^O(n) = \left[w_1^o(n), w_2^o(n), \cdots, w_k^o(n)\right]^T \quad (12)$$

$$\Theta^I(n) = \left[\theta_1^I(n), \theta_2^I(n), \cdots, \theta_k^I(n)\right]^T \quad (13)$$

where X(n) is input vector with size of l×1, the transpose of a vector is denoted by using the letter "T" in the superscript of the given vector, $W^I(n)$ is a matrix with the size of l×k while w_{ij} represents the connecting weights between the i^{th} node of the inputs and j^{th} node in the hidden layer, $\Phi^I(n)$ and $\Phi^O(n)$ are k×1 vectors express the input and output of hidden layer neurons, respectively. $W^O(n)$ indicates connecting weights between output layer and hidden layer. $\Theta^I(n)$ is a k×1 vector of input thresholds and θ(n) expresses the output threshold. $Y^I(n)$ represents the input value of the output neuron. The desired value and the final output of the network are denoted by d(n) and y(n), respectively. The Hyperbolic tangent function is the activation function of all hidden layer neurons. Hyperbolic tangent function and its derivation are expressed as:

$$\tanh(x) = \frac{e^x - e^{-x}}{e^x + e^{-x}} \quad (14)$$

$$\tanh'(x) = 1 - \left(\tanh(x)\right)^2 \quad (15)$$

where tanh'(x) denotes the derivation of hyperbolic tangent function.

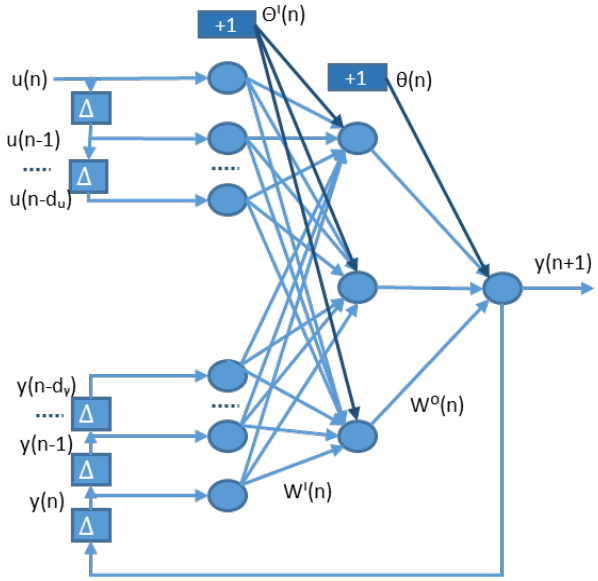

Fig 4. visualization of peak mapping.

The following are the steps for learning a network using the BP algorithm:

Step 1: Thresholds and Weights Initialization

Assign uniformly distributed, random, and small numbers to the parameters of weights and thresholds.

Step 2: Forward pass

Forward pass calculations which express the forward flow of the input signal are defined as following equations:

$$\Phi^{I}(n) = \left(W^{I}(n)\right)^{T} X(n) + \Theta^{I}(n) \quad (16)$$

$$\Phi^{O}(n) = \tanh(\Phi^{I}(n)) \quad (17)$$

$$Y^{I}(n) = \left(W^{O}(n)\right)^{T} \Phi^{O}(n) + \theta(n) \quad (18)$$

$$y(n) = \tanh(Y^{I}(n)) \quad (19)$$

which the linear combiner's output is written in the compact form.

Step 3: Backward pass (thresholds and weights update)

During the forward pass process, the output y(n) is calculated, which is an estimate of the value of the discriminator's output. Now this estimated value should be compared with the desired value. Then, based on the estimation error, the weights and thresholds of the network should be updated. Eq. (20) shows how to calculate the estimation error value.

$$J(n) = \frac{1}{2}\left(e(n)^{2}\right) = \frac{1}{2}\left(d(k) - y(k)\right)^{2} \quad (20)$$

The square of the output error is the objective function, which is minimized during the training process. Network weights and thresholds are updated by adding an adjustment value to each parameter.

4.2 Data Collection

The spoofing mitigation method based on NARX NN is verified using three spoofing data sets, 1, 2, and 3, in which the spoofing signal is combined with an authentic one. We used real GPS signal data that was free from any spoofing interference. Deceptive data were then generated by manipulating the samples of this dataset using software-based techniques. Fig. 5 illustrates how we generated a spoofing signal. The GPS antenna receives the authentic RF signal. Then, the RF signal passes through a band-pass filter and amplifier; it is down converted to the IF. The results are digitized and stored. Next, the authentic IF signal is delayed, then it is combined with the original one as a spoofing signal. A MATLAB-based GPS software receiver is utilized to process GPS data sets. The parameters of the software receiver are illustrated in Table 1.

Table 1. Parameters of the receiver.

Parameter	Value
Sampling frequency	4.09 MHz
Intermediate frequency	1.02 MHz
Bits of A/D	2 bit
Quantization levels	4
PLL damping ratio	0.7
DLL noise bandwidth	1 Hz
DLL damping ratio	0.7

5 Results discussion and performance evaluation

Matlab® R2016b is employed to train and test the NARX NN. Because each data set is 47 seconds long and the PRN code duration is 1 ms, the code discriminator unit produces 47,000 samples during the tracking process for each channel. The data sets were split 70% for training and 30% for testing.

The spoofing data is applied to the modified Software Defined Radio (SDR) receiver to evaluate the proposed mitigation method. The output of the correlators is initially passed through the spoofing detection unit in the modified SDR receiver, and if the spoofing signal is detected, the code discriminator unit switches to the NARX NN-based predictor to adjust the discriminator's output and update the local C/A code phase.

Offline processing of authentic and spoofing data sets is used to evaluate the proposed method. The location accuracy is measured in three states: (1) there is no spoofing signal and only the authentic signal is received (clean data set), (2) the receiver is under spoofing attack, and (3) the receiver is under spoofing attack while the proposed method for spoofing mitigation is in place.

The navigation results provided in the first case above, clean data set, serve as a reference point for measuring the accuracy of location measured in the other two cases.

Each scenario contains 1.9232e+11 IF signal samples and lasts 47 seconds. The solution period for navigation is 500 milliseconds. As a result, in each static scenario, the position is calculated 94 times. To calculate the amount of receiver location changes, we measure the RMS error of these 94 values relative to the reference point. The results are summarized in Table 2.

Columns two through five of Table 2 show positioning accuracy for the second case above, spoofing data sets, as the RMS error in the x, y, and z axes and the total error, respectively. Columns six through nine of Table 2 show the positioning accuracy for the third case above, in which the proposed method is used.

The proposed mitigation method's percentage improvement in location accuracy is expressed in the table's last column. As shown in the table, the average mitigation performance is 95.82%. Table 3 presents the mean and standard deviation of the positioning results. Positioning results on the map before and after mitigation method for data set 1, 2 and, 3 is shown in Figures 6, 7, and, 8, respectively

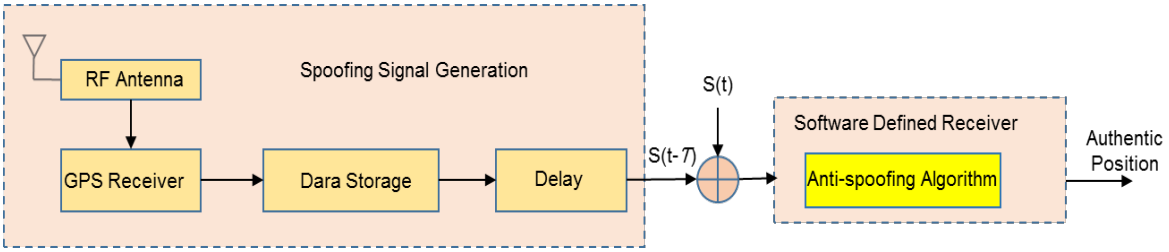

Fig 5. Block diagram of test setup.

Table 2. The performance of NARX NN-based spoofing mitigation technique.

Data set #	Before applying proposed method				After applying proposed method				Mitigation (%)
	RMS (m) x-axis	*RMS (m) y-axis*	*RMS (m) z-axis*	*RMS (m) total*	*RMS (m) x-axis*	*RMS (m) y-axis*	*RMS (m) z-axis*	*RMS (m) total*	
Data set 1	121.97	89.42	73.26	168.05	3.09	5.41	17.42	6.31	96.23
Data set 2	650.33	184.88	994.64	1202.67	91.20	52.24	77.81	105.11	91.25
Data set 3	15860	76401	62294	99846	17.37	26.02	1.60	31.31	99.96

Table 3. The mean and standard deviation of the positioning results.

Data set #	Before applying proposed method				After applying proposed method			
	Mean (m) x-axis	*Mean (m) y-axis*	*Mean (m) z-axis*	*STD total*	*Mean (m) x-axis*	*Mean (m) y-axis*	*Mean (m) z-axis*	*STD total*
Data set 1	3251845	3935787	3558006	1043.3	3251720	3935692	3557915	1476.6
Data set 2	3252373	3935882	3558927	1478	3251631	3935645	3557855	1476.3
Data set 3	3267583	4012098	3620227	1136	3251705	3935671	3557931	1477

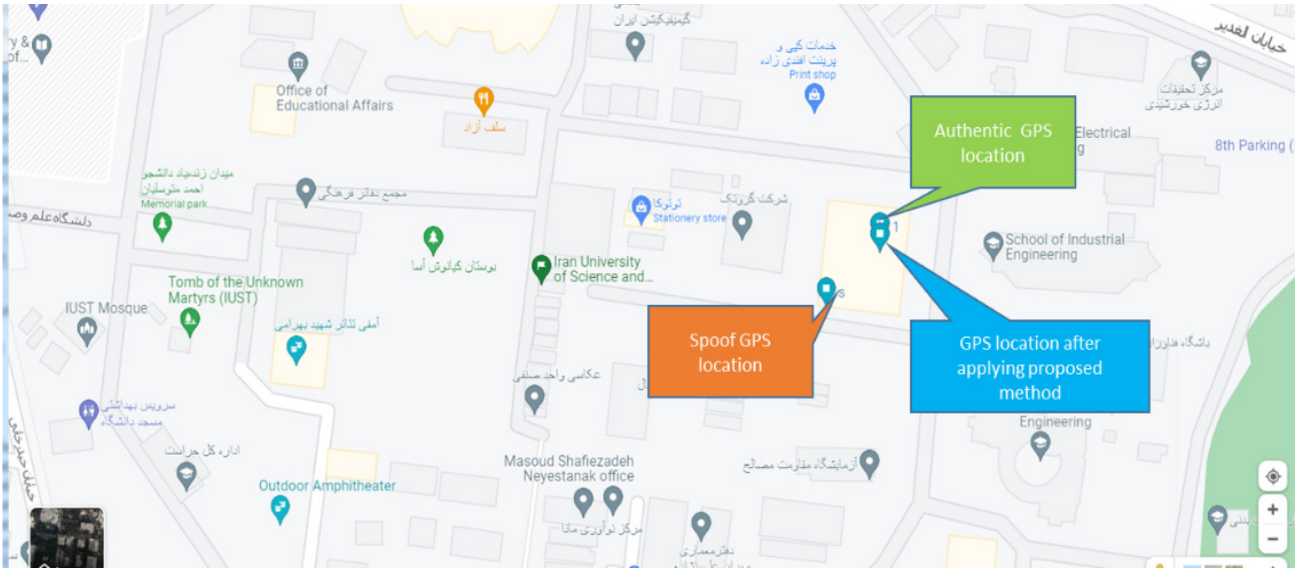

Fig 6. Positioning results on the map before and after mitigation method for data set 1.

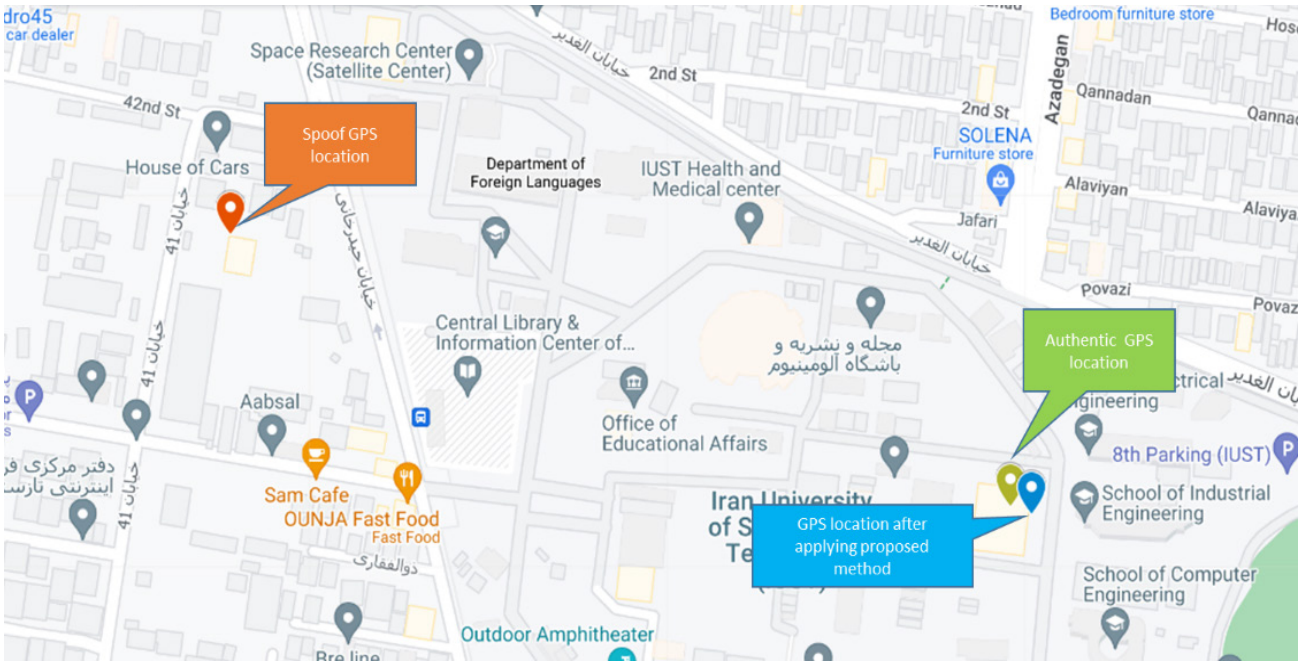

Fig 7. Positioning results on the map before and after mitigation method for data set 2.

Fig 8. Positioning results on the map before and after mitigation method for data set 3.

A further evaluation of the proposed method was carried out through the correlation coefficient (R) value that indicates the relationship between original data and predicted data associated with the code discriminator output. Figures 9 and 10 show a regression plot for train and test data, respectively.

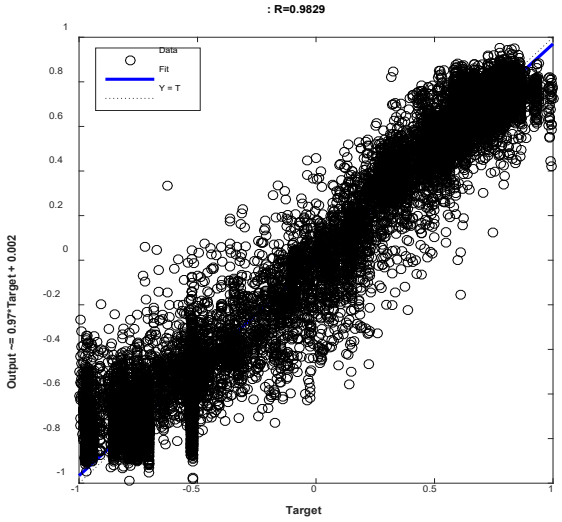

Fig 9. A regression plot for the train data.

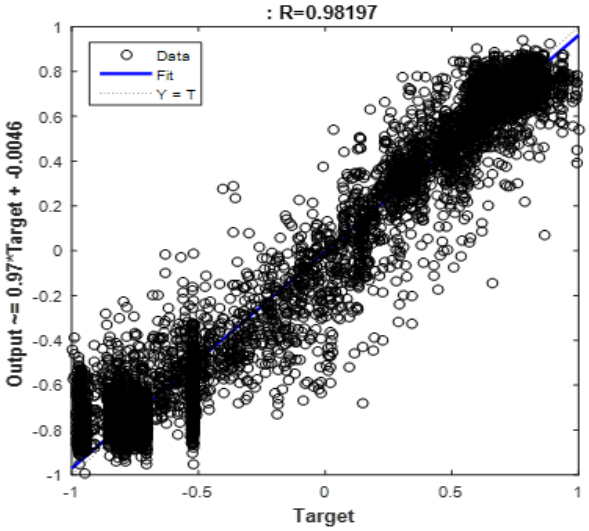

Fig 10. A regression plot for the test data.

R equals 0.9829 for training data and 0.9819 for testing data. The outcomes depicted in Fig. 8 show that the NARX modeling method created in the current study is a trustworthy method for modeling the code discriminator under spoofing attack conditions.

Table 4. Comparison of different anti-spoofing methods.

Methods	Technique	Spoofing feature	Advantages	Disadvantages	Position of applying algorithm	Implementation aspects
Spatial processing	Comparison of direction arrival [21]	Spoofing signals coming from the same direction	High-probability of detection	Extra hardware complexity and implementation	Incoming signal	Multiple receiver antennas
Correlation monitoring	Power-distortion detector [33]	Deviated shape of correlation function	Low-complexity	Inadequacy in multi-path and depend on previous information	Tracking - IF signal	Power monitoring and multiple correlator
TOA anomaly detection	Spoofing signal's inevitable delay [15]	Authentic/spoofing clock inconsistency	Low-complexity	Inefficient in synchronous attacks	Navigation	TOA analysis
Cryptographic techniques	Cryptographic authentication [13]	Not authenticated	High-effectiveness	Requires change in GPS signal structure	Navigation	Requires new GPS signals and services
Signal power anomaly detection	Absolute power monitoring [24]	Higher spoofing signal power	High-effectiveness	Inadequacy in the case of subtle attack scenario	IF signal	Absolute power Monitoring
Correlation monitoring based on artificial intelligence	Proposed method	Deviated shape of correlation function	Perform countermeasures against the spoofing attack	Performance is limited to carry-off spoofing attack	Tracking	Software upgrading

Finally, in Table 4 a qualitative comparison is provided to assess the benefits and drawbacks of the proposed method. The table contrasts the methods introduced in the literature review with the current procedure.

6 Conclusion

In this paper, an artificial intelligence technique was used to help the GPS receiver's code tracking loop deal with a carry-off spoofing attack. Because the carry-off spoofing signal is so similar to the original GPS signal, it can interfere with the receiver's tracking loop without unlocking it. The discriminator is an essential part of the tracking loop, whose function is effective in replacing the authentic signal with the fake signal. We added a NARX NN to the discriminator unit in this study to predict the correct discriminator's output values when the spoofing attack occurs. The R value, which represents the relationship between the original and predicted data, was computed. For training data, R equals 0.9829, and for testing data, R equals 0.9819. The NN's reliance on training data, which consists of authentic signal features, is an advantage that allows it to predict the correct values. The proposed method was tested on three spoofing data sets, and the results showed that it was 95.82% capable of mitigating the carry-off spoofing attack.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

S. Tohidi: Conceptualization, Methodology, Software, Data curation, Visualization, Investigation, Original draft preparation. **M. R. Mosavi**: Supervision, Investigation, Reviewing and editing.

Funding

No funding was received for this work.

Acknowledgements

This work is based upon research supported by Iran National Science Foundation (INSF) and under project No.4023276.

Informed Consent Statement

Not applicable.

References

[1] L. Bai, C. Sun, A. G. Dempster, H. Zhao and W. Feng, "GNSS spoofing detection and mitigation with a single 5G base station aiding," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 60, no. 4, pp. 4601-4620, Aug. 2024.

[2] P. Borhani-Darian, H. Li, P. Wu, and P. Closas, "Detecting GNSS spoofing using deep learning," *EURASIP Journal on Advances in Signal Processing*, vol. 14, 2024.

[3] A. Iqbal, N. A. Muhammad, and S. Biplab, "A deep learning based induced GNSS spoof detection framework," *IEEE Transactions on Machine Learning in Communications and Networking*, vol. 2, pp. 457-478, 2024.

[4] K. Radoš, M. Brkić, and D. Begušić, "Recent advances on jamming and spoofing detection in GNSS," *Sensors*, vol. 24, no. 13, pp. 4210, 2024.

[5] L. Bai, C. Sun, A. G. Dempster, H. Zhao and W. Feng, "GNSS spoofing detection and mitigation with a single 5G base station aiding," in *IEEE Transactions on Aerospace and Electronic Systems*, vol. 60, no. 4, pp. 4601-4620, Aug. 2024.

[6] X. Shang, F. Sun, B. Liu, L. Zhang and J. Cui, "GNSS spoofing mitigation with a mult correlator estimator in the tightly coupled INS/GNSS integration," in *IEEE Transactions on Instrumentation and Measurement*, vol. 72, pp. 1-12, 2023.

[7] G. Michieletto, F. Formaggio, A. Cenedese and S. Tomasin, "Robust localization for secure navigation of UAV formations under GNSS spoofing attack," in *IEEE Transactions on Automation Science and Engineering*, vol. 20, no. 4, pp. 2383-2396, Oct. 2023.

[8] F. Rothmaier, Y. Chen, S. Lo, T. Walter, "GNSS spoofing mitigation in the position domain," *Proceedings of the 2021 International Technical Meeting of The Institute of Navigation*, January 2021, pp. 42-55, 2021.

[9] B. Yang, M. Tian, Y. Ji, J. Cheng, Z. Xie and S. Shao, "Research on GNSS spoofing mitigation technology based on spoofing correlation peak cancellation," in *IEEE Communications Letters*, vol. 26, no. 12, pp. 3024-3028, Dec. 2022.

[10] K. Ghorbani, N. Orouji, and M. R. Mosavi, "Navigation message authentication based on one-way hash chain to mitigate spoofing attacks for GPS ll," *Wireless Personal Communications*, vol. 113, no. 4, pp. 1743-1754, 2020.

[11] A. S. Musleh, G. Chen, and Z. Y. Dong, "A survey on the detection algorithms for false data injection attacks in smart grids," *IEEE Transactions on Smart Grid*, vol. 11, no. 3, pp. 2218-2234, 2019.

[12] B. Motella, M. Nicola, and S. Damy, "Enhanced GNSS authentication based on the joint CHIMERA/OSNMA scheme," *IEEE Access*, vol.

9, pp. 121570-121582, 2021.

[13] Z. Wu, C. Liang, and Y. Zhang, "Blockchain-based authentication of GNSS civil navigation message," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 59, pp. 4380-4392, 2023.

[14] G. Seco-Granados, D. Gómez-Casco, J. A. López-Salcedo, and I. Fernández-Hernández, "Detection of replay attacks to GNSS based on partial correlations and authentication data unpredictability," *GPS Solutions*, vol. 25, no. 2, p. 33, 2021.

[15] V. Truong, A. Vervisch-Picois, J. Rubio Hernan, and N. Samama, "Characterization of the ability of low-cost GNSS receiver to detect spoofing using clock bias," *Sensors*, vol. 23, pp. 2735, 2023.

[16] F. Rothmaier, Y. H. Chen, S. Lo, and T. Walter, "GNSS spoofing detection through spatial processing," *Navigation*, vol. 68, no. 2, pp. 243-258, 2021.

[17] J. Magiera, "A multi-antenna scheme for early detection and mitigation of intermediate GNSS spoofing," *Sensors*, vol. 19, no. 10, p. 2411, 2019.

[18] S. H. Seo, B. H. Lee, S. H. Im, G. I. Jee, and K. S. Kim, "Efficient spoofing identification using baseline vector information of multiple receivers," *GPS Solutions*, vol. 22, pp. 1-14, 2018.

[19] A. Broumandan, A. Jafarnia-Jahromi, S. Daneshmand, and G. Lachapelle, "Effect of tracking parameters on GNSS receivers' vulnerability to spoofing attack," *Proceedings of the 29th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2016)*, pp. 3033-3043, 2016.

[20] A. Broumandan, A. Jafarnia-Jahromi, S. Daneshmand, and G. Lachapelle, "Overview of spatial processing approaches for GNSS structural interference detection and mitigation," *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1246-1257, 2016.

[21] S. Li, H. Lin, X. Tang and F. Wang, "Blind spoofing detection for anti-jamming multiantenna GNSS receivers," *IEEE Sensors Journal*, vol. 24, pp. 39418-39431, 2024.

[22] M. L. Psiaki, S. P. Powell, and B. W. O'Hanlon, "GNSS spoofing detection using high-frequency antenna motion and carrier-phase data," *Proceedings of the 26th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2013)*, pp. 2949-2991, 2013.

[23] Q. Wang, Y. Yang, A. Liu, and P. Fan, "Vehicle mounted single-antenna GNSS spoofing detection method based on motion trajectory," *GPS Solutions*, vol. 28, pp.155, 2024.

[24] L. Zhang, W. Lu, W. Renbiao, and Z. Xuebin, "A new approach for GNSS spoofing detection using power and signal quality monitoring," *Measurement Science and Technology*, vol. 35, 126109, 2024.

[25] D. P. Shepard and T. E. Humphreys, "Characterization of receiver response to a spoofing attack," *Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2011),* 2011, pp. 2608-2618.

[26] A. Jafarnia Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "GPS spoofer countermeasure effectiveness based on signal strength, noise power, and C/N_0 measurements," *International Journal of Satellite Communications and Networking*, vol. 30, no. 4, pp. 181-191, 2012.

[27] A. Cavaleri, B. Motella, M. Pini, and M. Fantino, "Detection of spoofed GPS signals at code and carrier tracking level," *5th IEEE ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC)*, pp. 1-6, 2010.

[28] B. M. Ledvina, W. J. Bencze, B. Galusha, and I. Miller, "An in-line anti-spoofing device for legacy civil GPS receivers," *Proceedings of the 2010 International Technical Meeting of the Institute of Navigation*, pp. 698-712, 2010.

[29] K. D. Wesson, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "An evaluation of the vestigial signal defense for civil GPS anti-spoofing," *Proceedings of the 24th International Technical Meeting of the Satellite Division of the institute of navigation (ION GNSS 2011)*, pp. 2646-2656, 2011.

[30] M. Pini, M. Fantino, A. Cavaleri, S. Ugazio, and L. L. Presti, "Signal quality monitoring applied to spoofing detection," *Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2011)*, pp. 1888-1896, 2011.

[31] A. Broumandan, A. Jafarnia-Jahromi, G. Lachapelle, and R. T. Ioannides, "An approach to discriminate GNSS spoofing from multipath fading," *8th IEEE ESA Workshop on Satellite Navigation Technologies and European Workshop*

on GNSS Signals and Signal Processing (NAVITEC), pp. 1-10, 2016.

[32] A. Pirsiavash, A. Broumandan, and G. Lachapelle, "Two-dimensional signal quality monitoring for spoofing detection," *Proceedings of the ESA/ESTEC NAVITEC 2016 Conference, Noordwijk, The Netherlands*, pp. 14-16, 2016.

[33] J. N. Gross, C. Kilic, and T. E. Humphreys, "Maximum-likelihood power-distortion monitoring for GNSS-signal authentication," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 55, no. 1, pp. 469-475, 2018.

[34] K. Borre, D. M. Akos, N. Bertelsen, P. Rinder, and S. H. Jensen, "A software-defined GPS and Galileo receiver: a single-frequency approach," Springer Science & Business Media, 2007.

[35] S. Tohidi and M. R. Mosavi, "GNSS spoofing detection using a fuzzy classifier based on time–frequency analysis of the autocorrelation function," *GPS Solutions*, vol. 28, no. 3, pp. 146, 2024.

[36] T. Lin, B. G. Horne, P. Tino, and C. L. Giles, "Learning long-term dependencies in NARX recurrent neural networks," *IEEE Transactions on Neural Networks*, vol. 7, no. 6, pp. 1329-1338, 1996.

[37] E. Cadenas, W. Rivera, R. Campos-Amezcua, and C. Heard, "Wind speed prediction using a univariate ARIMA model and a multivariate NARX model," *Energies*, vol. 9, no. 2, p. 109, 2016.

[38] T. Zhang, R. Barthorpe, and K. Worden, "On treed gaussian processes and piecewise-linear NARX modelling," *Mechanical Systems and Signal Processing*, vol. 144, p. 106877, 2020.

[39] E. Diaconescu, "The use of NARX neural networks to predict chaotic time series," *WSEAS Transactions on Computer Research*, vol. 3, no. 3, pp. 182-191, 2008.

[40] E. Shafiee, M. R. Mosavi, and M. Moazedi, "Detection of spoofing attack using machine learning based on multi-layer neural network in single-frequency GPS receivers," *The Journal of Navigation*, vol. 71, no. 1, pp. 169-188, 2018.

Biographies

S. Tohidi received her B.Sc. and M.Sc. degrees in Electronic Engineering from respectively Shahid Beheshti University and Malek Ashtar University of Technology, Tehran, Iran. She is currently a Ph.D. Student in the Department of Electrical Engineering at Iran University of Science and Technology. Her research interests include signal processing, artificial intelligence, and GPS applications.

M. R. Mosavi received his B.Sc., M.Sc., and Ph.D. degrees in Electronic Engineering from Iran University of Science and Technology (IUST), Tehran, Iran in 1997, 1998, and 2004, respectively. He is currently a faculty member (Full Professor) of the Department of Electrical Engineering of IUST. He is the author of more than 600 scientific publications in journals and international conferences in addition to 15 academic books. His research interests include circuits and systems design. He is also editor in-chief of "Iranian Journal of Marine Technology" and editorial board member of "Iranian Journal of Electrical and Electronic Engineering" and "GPS Solutions".