



A multi-layer perceptron neural network to mitigate the interference of time synchronization attacks in stationary GPS receivers

N. Orouji¹ · M. R. Mosavi¹

Received: 6 October 2020 / Accepted: 25 March 2021 / Published online: 5 April 2021
© The Author(s), under exclusive licence to Springer-Verlag GmbH Germany, part of Springer Nature 2021

Abstract

Accurate timing is one of the key features of the Global Positioning System (GPS), which is employed in many critical infrastructures. Any imprecise time measurement in GPS-based structures, such as smart power grids, economic activities, and communication towers, can lead to disastrous results. The vulnerability of the stationary GPS receivers to the time synchronization attacks (TSAs) jeopardizes the GPS timing precision and trust level. In the past few years, studies suggested the adoption of estimators to follow the authentic trend of the clock offset information under attack conditions. However, the estimators would lose track of the authentic signal without proper knowledge of the signal characteristics. Therefore, a multi-layer perceptron neural network (MLP NN) is proposed to follow the trend of the data. The main difference between the proposed method and typical estimators is the reliance of the network on the training information consisting of signal features. The proposed MLP NN performance has been evaluated through two real-world datasets and two well-known types of TSA. The root mean square error results exhibit an improvement of at least six times compared to other conventional and state-of-art methods.

Keywords GPS spoofing attacks · MLP NN · Error estimation · Robust receiver · Clock offset

Introduction

The Global Positioning System (GPS) provides accurate timing information for time-dependent structures such as financial markets and banking systems, communication networks, and phasor measurement units (PMUs). For instance, GPS offers a precision better than 1 μ s for PMUs to maintain the high sampling rate of the unit (Xie and Meliopoulos 2020). The weak nature of GPS signals causes vulnerability to all kinds of environmental conditions, and its well-known civilian structure is prone to intentional interferences. Therefore, a malicious signal with slightly higher strength can outperform the authentic signal effortlessly (Bonebrake and O'Neil 2014).

Customarily, the receivers that exploit the timing information of the GPS signal are stationary; thus, they are threatened more by a specific category of spoofing attacks: time synchronization attack (TSA). TSA manipulates the signal information so that the receiver miscalculates the clock offset and causes erroneous time measurement (Shepard et al. 2012). Generally, in this type of attack, the position of the receiver will remain intact. Wrong or inaccurate time stamps in PMU measurements can cause false alarms or prevent the disclosure of an event in the network (Jiang et al. 2013). A similar attack on the communication towers can disturb time synchronization of adjacent towers, and eventually, jam their signals (3GPP2 2004).

An intermediate spoofer device contains a receiver and is placed near the target; thus, it spreads intelligently altered signals very similar to the authentic one in Doppler frequency and code phase (Mosavi et al. 2017). Therefore, the spoofing detection methods in the acquisition stage would be ineffective. TSA is considered as an intermediate spoofing attack, and software-defined radios (SDRs) can implement them straightforwardly (Schmidt et al. 2019). SDRs are accessible for public use; therefore, the generation of TSA is feasible and cost-effective, considering that

✉ M. R. Mosavi
M_Mosavi@iust.ac.ir

N. Orouji
Nilloofar_Orouji@elec.iust.ac.ir

¹ Department of Electrical Engineering, Iran University of Science and Technology, 16846-13114 Narmak, Tehran, Iran

most commercial receivers cannot detect intermediate or even simplistic attacks (Schmidt et al. 2020).

A vast number of countermeasures and protection techniques have been proposed to detect or mitigate the effects of TSA, which can be categorized into four classes (Schmidt et al. 2016). The first category includes signal processing methods that monitor and analyze the signal features for any unexpected anomalies in quality, power, or any other observable parameters (Zhang and Zhan 2016; Schmidt et al. 2020). Multi-antenna receivers and radio spectrum inspections are organized in the second category and exploit the angle of arrival of each signal to detect the direction of its source (Magiera 2019; Heng et al. 2014). The cryptographic techniques present solutions in the third category that relies on the next-generation GPS signal structure (Ghorbani et al. 2020) or the relation between military signals and authentic ones to detect the invasion (Psiaki et al. 2013). The last category suggests the correlation of GPS information with other time sources, such as GLONASS (Mosavi et al. 2016).

Cryptographic techniques are resilient to intermediate and advanced spoofing attacks; however, they are prone to simplistic attacks such as meaconing (Ghorbani et al. 2020). Therefore, it is strongly suggested to exploit the method accompanying other defense solutions to achieve the maximum level of protection (Musleh et al. 2019). The facility of cryptography is only available on new GPS signals and services (GPS CNAV) and the Galileo system, which is not exploited extensively.

As an advantage, there is no requirement to modify the signal protocols or the satellites for the validation of the GPS information by the other GNSS or data sources. However, the network-based validation creates an overwhelming amount of data traffic through the network and is vulnerable to cyber attacks, such as man-in-the-middle. Furthermore, verification of the information with other satellite systems requires extra receivers, which is not very cost-efficient. The immunity of multi-antenna defenses to SDR-generated attacks and their intrinsic resistance to spoofing distinguish them as a robust choice for secure receivers. Still, the utilization of multi-antenna receivers and radio spectrum analyses are quite costly.

The signal processing countermeasures can be applied to the receivers by updating their firmware and equipping them with the latest defense methods. However, they do not require any hardware modifications or adjustments in signal structure. This research contributes a spoof-detection and mitigation algorithm based on the clock offset observations, which lies within the mentioned category. A multi-layer perceptron neural network (MLP NN) is trained to follow the behavior of clock offset information and maintain the authentic trend under TSA conditions. The network reduces the diversions introduced in the information and represents

an acceptable accuracy for PMUs, the communication towers, and other time-dependent applications.

The contributions of this research can be listed as follows:

- A three-layer MLP NN is proposed, which can impressively mimic the clock offset trend. Since each dataset has a similar pattern as the other ones in terms of clock offset behavior, the network is trained once, and there is no necessity to train it with every new dataset.
- A reference dataset can be exploited to train the network in offline mode; therefore, there is no obligation to train the network in the setup stage of the receiver. Furthermore, the trained weights can be stored in the memory of the receiver and exploited at each startup.
- The defensive mechanism of the proposed method is independent of the generation procedure of TSA, and it only concentrates on the correction of destructive effects on the clock offset. Therefore, it can cover a vast number of TSAs that influence the clock offset information, without concern about new or future methods of attack generation.
- The proposed MLP NN is exploited in a detection algorithm, which can detect the type of attack.
- The algorithm requires low memory space, and it does not demand complicated mathematical tools and a massive number of computational resources. Therefore, the update of the receiver firmware consists of a few lookup tables and the algorithm routine.

The following section reviews clock offset derivation and the state-of-art algorithms in signal-processing defense techniques. The configurations of the MLP NN and the algorithm are expressed in the third section, and it will be followed by experimental results, which are obtained by two real datasets. Finally, the conclusions are made in the last section.

Terminology review and related works

The first part of this section explains the procedure of clock offset calculations and its associated terminology. The second part discusses the existing solutions to confront the threat of TSA in stationary receivers and inspects their cons and pros.

GPS time and clock offset derivation

Generally, the GPS signals are exploited to determine the position, velocity, and time or PVT solution of the receiver. The position accuracy in open sky conditions is about 4.9 m for smartphones (Diggelen and Enge 2015). Though, depending on environmental conditions, the accuracy will be reduced

in more challenging situations. According to the studies of Lewandowski et al. (1993), the precision of time measurements of GPS receivers is in the order of nanoseconds (Li et al. 2015).

The GPS signals received at the front end of the receiver will be passed through acquisition, tracking, and navigation data processing stages to derive the PVT information. Based on the retrieved information, the position of each satellite is calculated, and the pseudoranges are estimated as well. Pseudoranges assist in computing the PVT solution. The relationship connecting the trip time between the k th satellite and the user’s receiver, denoted by τ_u^k , the speed of light c , and the corresponding pseudorange ρ_u^k , is defined as (Borre et al. 2007):

$$t_u - t^k = \tau_u^k = \frac{\rho_u^k}{c} \tag{1}$$

where t_u is the user time and t^k is the k th satellite time. Consider t^{GPS} as absolute GPS time. Clocks of the receiver and satellites are not exactly the same as the GPS time. Therefore, the time of the user and k th satellite are expressed as follows:

$$t_u = t^{\text{GPS}} + dt_u \tag{2}$$

$$t^k = t_u^{\text{GPS}} - \tau_u^{k,\text{GPS}} + dt^k \tag{3}$$

where the epoch time, which expressed in terms of the receiver clock, is t_u , and ρ_u^k is known from the observations. According to (1), t^k can be calculated and corrected with satellite clock offset dt^k . Now the transmit time is obtained in absolute GPS time as well as clock offset of the user dt_u .

TSA formation and countermeasures

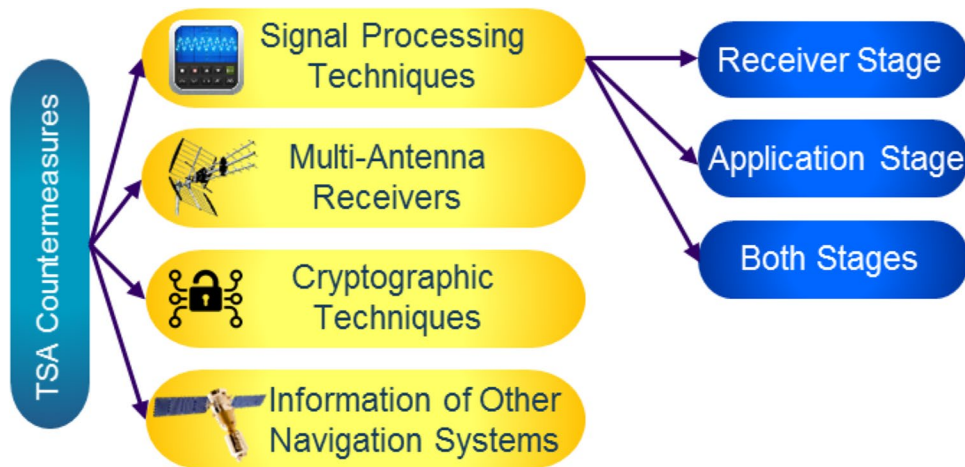
The clock offset of receiver dt_u is prone to TSA attacks. Any distortion in the receiver clock offset directly influences

the receiver clock and will be resulted in erroneous time stamps for data measurement or corruption of the synchronization between devices. The mentioned distortion can be conducted by any possible means, such as a fluctuation in pseudorange or modification in ephemeris information. In Jiang et al. (2013), a TSA optimization problem is formulated to increase the clock offset error, and consequently, the phase measurement error in a PMU. The problem conditions are precisely selected so that the position of the receiver and satellites, and pseudoranges are not altered drastically. These conditions develop a hard-to-detect TSA for simplistic observation countermeasures, such as position monitoring.

Another spoofing scheme is proposed by Lee et al. (2019) and Schmidt et al. (2020) that injects a malicious signal to the pseudorange measurements. Based on the shape of the added signal, two types of TSAs are introduced. In the first type of the proposed TSA, a step-shaped signal is added abruptly to the authentic measurements, while the second type of attack consists of gradual modification of the clock offset. The location of the receiver is constant, and its velocity is assumed to be zero in these cases.

The countermeasures for such attacks, independent of their configuration scheme, are divided into three categories: exploiting a defense mechanism in the receiver stage, detection or mitigating the attack effects on the application stage, or a combination of both methods, as shown in Fig. 1. Most of the countermeasures in the application stage detect the attack based on the unusual status of the device or the network. The application of GPS timing in PMUs and their vulnerability to TSA have drawn attention to the issue. Therefore, various pieces of research have been conducted on this specific application and provided many solutions for TSA detection or mitigation in the application layer. In Zhu et al. (2016), the number of visible satellites has been estimated, and modifications in the signal were observed and investigated. Similarly, Wang and Chakraborty (2016) monitor the oscillations in the network and check the consistency of parameter updates in

Fig. 1 Defenses against TSAs are categorized into four classes, in which signal processing techniques are utilized in the stages of the receiver, application, or both



each network node in a distributed scheme. The evaluation of the network time integrity and tracking the signal quality in Riedel et al. (2019) is an instance of exploiting both receiver-level and application-level defense mechanisms.

Many solutions exclusively detect the malicious invasion based on statistical estimations, and the supervisor will conduct further reactions, such as disconnecting the faulty PMU. However, some defense mechanisms are equipped with error correction and mitigation techniques. Statistical model and state estimation techniques have been utilized for synchrophasor data correction in Fan et al. (2018a), while Fan et al. (2018b) employ the analysis of the network matrices to estimate the phase shift, which is generated by the attack, and determination of the infected PMU. Furthermore, the Supervisory Control and Data Acquisition (SCADA) system and PMU measurements assist a dynamic filter to estimate the phase shift of the attack in Siamak et al. (2020). The method also corrects the faulty measurements of the attacked PMU. These kinds of techniques explore the network models with complex relationships and investigate the results of spreading erroneous measurements through the network, which can eventually endanger the network state.

A more desirable method is the detection of attack in the receiver stage and refining the time information before exploiting them in the application. TSA rejection and mitigation (TSARM) technique employs the spoofing attack model and mitigates the attack effects by correcting the pseudoranges and their rates (Khalajmehrabadi et al. 2018a, b). A belief propagation technique and adaptive extended Kalman filter (EKF) are utilized to adjust the pseudorange measurements in Bhamidipati et al. (2019), and the receivers are also equipped with multiple directional antennas. Low-memory and robust estimator (RE) is also proposed in Lee et al. (2019), which mitigates the TSA impacts effectively and does not require any parameter tuning procedure.

All of the mentioned contributions effectively mitigate the TSA effects; however, they follow specific modifications in the signal to alleviate the attack outcomes. Furthermore, the accuracy of the methods is an important issue, which will be addressed in the next sections. The contribution of this research is a MLP network that focuses on the time information correction in the receiver level, independent of how the attack generated or affected the other parameters to alter the time. Therefore, in the upcoming section, the basics of the MLP NN will be discussed briefly and the correction mechanism explained in detail.

An MLP NN for spoof mitigation: basics and mechanism

Multi-layer feedforward networks constitute one of the highly popular categories of NNs. They are called feedforward since the input signal propagates through the structure, which can have one or more hidden layers in a forward direction. Commonly, these networks, which are referred to as MLP NNs, can provide solutions for a diverse range of complex problems after receiving the proper training. The error back-propagation (BP) algorithm is employed to train MLP NNs in a supervised routine and consists of two passes: forward pass and backward pass (Haykin 2009). During the forward pass, the response of each layer to the input signal is investigated precisely, while the network weights remain constant. In the backward pass, the error is attained by the difference between the resultant output and the desired value. The error is exploited to adjust the weights and thresholds. Achieving the minimum possible error with a reasonable number of iterations is the ultimate goal of the learning process (Mosavi and Shafiee 2016).

In this section, a three-layer MLP NN is proposed and trained by the error BP algorithm in a supervised manner. Generally, the NNs are expressed by the number of neurons in each layer. For instance, a network with p nodes in the input layer, q neurons in the hidden layer, and r neurons in the output layer is denoted by $N(p, q, r)$. According to this notation, in the first subsection, the calculations of the BP algorithm are presented for the $N(p, q, 1)$ network, and in the second subsection, the proposed network structure with $N(3, 3, 1)$ is discussed.

Network training based on BP algorithm

Consider an $N(p, q, 1)$ network, as depicted in Fig. 2. Network parameters are defined as:

$$X(k) = [x_1(k), x_2(k), \dots, x_p(k)] \quad (4)$$

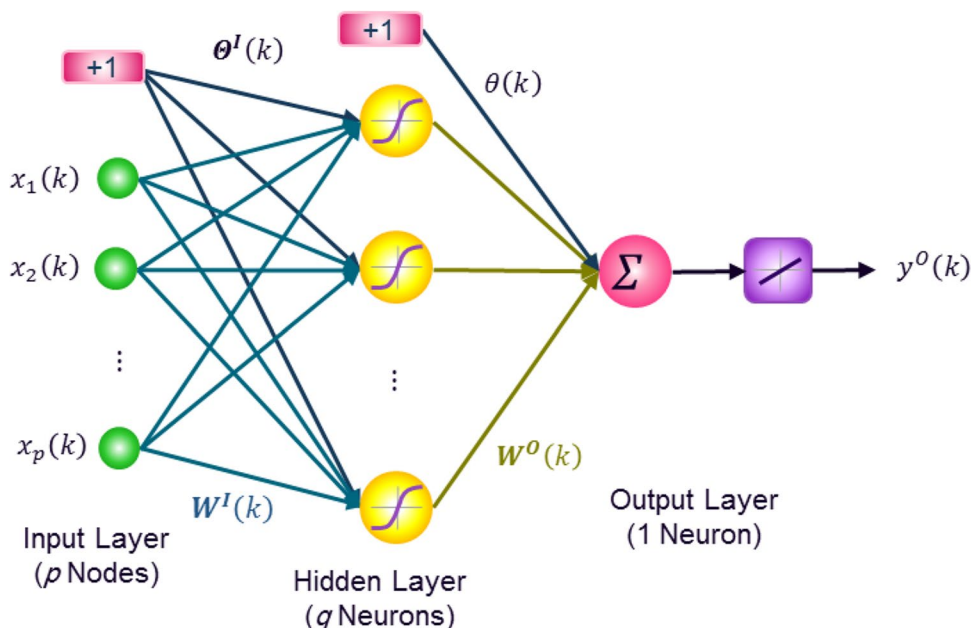
$$W^I(k) = \begin{bmatrix} w_{11}^I(k) & \dots & w_{1q}^I(k) \\ \vdots & \ddots & \vdots \\ w_{p1}^I(k) & \dots & w_{pq}^I(k) \end{bmatrix} \quad (5)$$

$$\Theta^I(k) = [\theta_1(k), \theta_2(k), \dots, \theta_q(k)] \quad (6)$$

$$W^O(k) = [w_1^O(k), w_2^O(k), \dots, w_q^O(k)] \quad (7)$$

$$V^I(k) = [v_1^I(k), v_2^I(k), \dots, v_q^I(k)] \quad (8)$$

Fig. 2 General form of $N(p, q, 1)$ network is illustrated, consisting of an input layer with p nodes, a hidden layer containing q neurons, and a single output layer



$$Y^I(k) = [y_1^I(k), y_2^I(k), \dots, y_q^I(k)] \tag{9}$$

where $X(k)$ is a $p \times 1$ input vector, $W^I(k)$ is the input weights matrix with the size of $p \times q$, $\theta^I(k)$ expresses a $q \times 1$ vector of input thresholds, $W^O(k)$ indicates output weight vector with the size of $q \times 1$, and $\theta(k)$ is the output threshold. The stimulation of neurons in the hidden layer is denoted by a $q \times 1$ vector $V^I(k)$, and the stimulation of output layer neuron is denoted by $v^O(k)$ (Mosavi 2006). Output of hidden layer neurons is a $q \times 1$ vector $Y^I(k)$.

The final output of the network and desired value are denoted by $y^O(k)$ and $d(k)$, respectively. The activation function of each neuron is a sigmoid function. The function and its derivation are presented as:

$$\sigma(x) = \frac{2}{1 + e^{-2x}} - 1 \tag{10}$$

$$\sigma'(x) = \sigma(x)(1 - \sigma(x)) \tag{11}$$

where $\sigma'(x)$ denotes the derivation of sigmoid. The following steps express the procedure of network learning by the BP algorithm:

Step 1: Initialization of the weights and thresholds

Assign small, random, and uniformly distributed numbers to the corresponding parameters.

Step 2: Forward pass

Forward calculations, based on Fig. 2, are defined as:

$$v_j^I(k) = \sum_{i=1}^p x_i(k)w_{ji}^I(k) + \theta_j^I(k) \tag{12}$$

$$y_j^I(k) = \sigma_j(v_j^I(k)) \tag{13}$$

$$v^O(k) = \sum_{i=1}^q y_i^I(k)w_i^O(k) + \theta(k) \tag{14}$$

$$y^O(k) = \sigma(v^O(k)) \tag{15}$$

which express the forward flow of the input signal.

Step 3: Backward pass (weights and thresholds update)

After obtaining the relationships between inputs and output, the result should be compared with the desired signal. The objective function based on the squared error is defined as:

$$J(k) = \frac{1}{2}(e(k)^2) = \frac{1}{2}(d(k) - y^O(k))^2 \tag{16}$$

where $e(k)$ is the output error. In each iteration, the algorithm endeavors to minimize the function by updating the adaptable parameters. The updating process is operated by adding

an adjustment value to each parameter. For instance, the update relation for $w_j^O(k)$ is expressed as:

$$w_j^O(k + 1) = w_j^O(k) + \Delta w_j^O(k) \tag{17}$$

where $\Delta w_j^O(k)$ is the adjustment value and determined by partial derivative of $J(k)$ with respect to $w_j^O(k)$:

$$\Delta w_j^O(k) = -\eta \frac{\partial J(k)}{\partial w_j^O(k)} = \eta \cdot e(k) \cdot \sigma(v^O(k)) \cdot (1 - \sigma(v^O(k))) \cdot y_j^I(k) \tag{18}$$

in which η is the learning rate parameter that influences on convergence speed of the algorithm. Likewise, the adjustment values for other parameters of the network are expressed as:

$$\Delta \theta(k) = -\eta \frac{\partial J(k)}{\partial \theta(k)} = \eta \cdot e(k) \cdot \sigma(v^O(k)) \cdot (1 - \sigma(v^O(k))) \tag{19}$$

$$\Delta w_{ji}^I(k) = -\eta \frac{\partial J(k)}{\partial w_{ji}^I(k)} = \eta \cdot e(k) \cdot \sigma'(v^O(k)) \cdot w_j^O(k) \cdot \sigma_j'(v_j^I(k)) \cdot x_i(k) \tag{20}$$

$$\Delta \theta_j^I(k) = -\eta \frac{\partial J(k)}{\partial \theta_j^I(k)} = \eta \cdot e(k) \cdot \sigma'(v^O(k)) \cdot w_j^O(k) \cdot \sigma_j'(v_j^I(k)) \tag{21}$$

which can be exploited to update parameters in each iteration.

Step 4: Iteration

The time instant k is increased, and the algorithm is repeated from Step 2 until the output error conditions satisfy.

Proposed network structure

The ultimate goal of TSA is to affect the clock offset information and cause errors in time stamps; therefore, an MLP NN can be a great help to estimate the authentic trend of the clock offset and preserve the receiver from the catastrophic consequences of TSA. The efficient utilization of MLP NN requires a proper selection of the network features, such as type of architecture, the number of layers and neurons, and training algorithm. Generally, the optimal decisions are made through a trial-and-error procedure (Shafiee et al. 2018). In the proposed network, the previous samples of the clock offset are employed as inputs to predict the upcoming one.

The decision is directed by considering the trade-off between computational complexity and mean square error (MSE) of the training process. The network complexity directly relates to its order and depends on the number of

weights and thresholds. The order of a general $N(p, q, I)$ network is defined as (Karim 2019; Haykin 2009):

$$\text{Network Order} = (p + 2)q + 1 \tag{22}$$

which has a direct relation with the dimensions of the network.

Multiple experiments have been conducted, and the number of neurons and inputs varied between two and 20 to determine the optimal selections. Furthermore, different activation functions such as Gaussian functions with various means and standard deviations are employed to attain the best solution. The sigmoid function is a popular selection as an activation function, and it performs well in estimating the clock offset trend. The final structure selection of the network has been established based on the results of Fig. 3. According to the figure, NNs with three inputs have lower MSEs in comparison with others. Specifically, networks with three and four neurons have the lowest possible MSEs. In terms of epochs, networks with four inputs have the fastest convergence rate. However, due to the nature of spoofing problems, the MSE parameter is a more crucial decision point than the convergence rate. Based on the mentioned priorities and tendency for simplicity, the $N(3, 3, 1)$ network with sigmoid activation functions, which is depicted in Fig. 4, is selected to estimate the clock offset trend. As shown in the figure, the inputs of the network are three previous samples of the clock offset information, which are $d(k - 1)$, $d(k - 2)$, and $d(k - 3)$. Consequently, the output

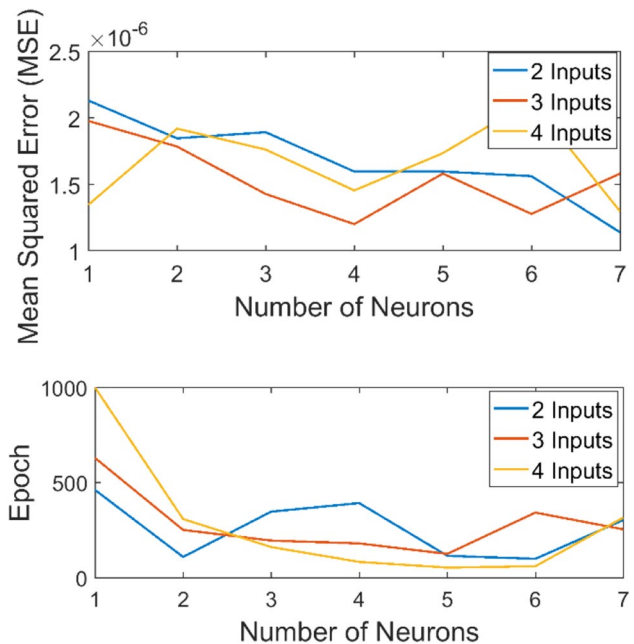
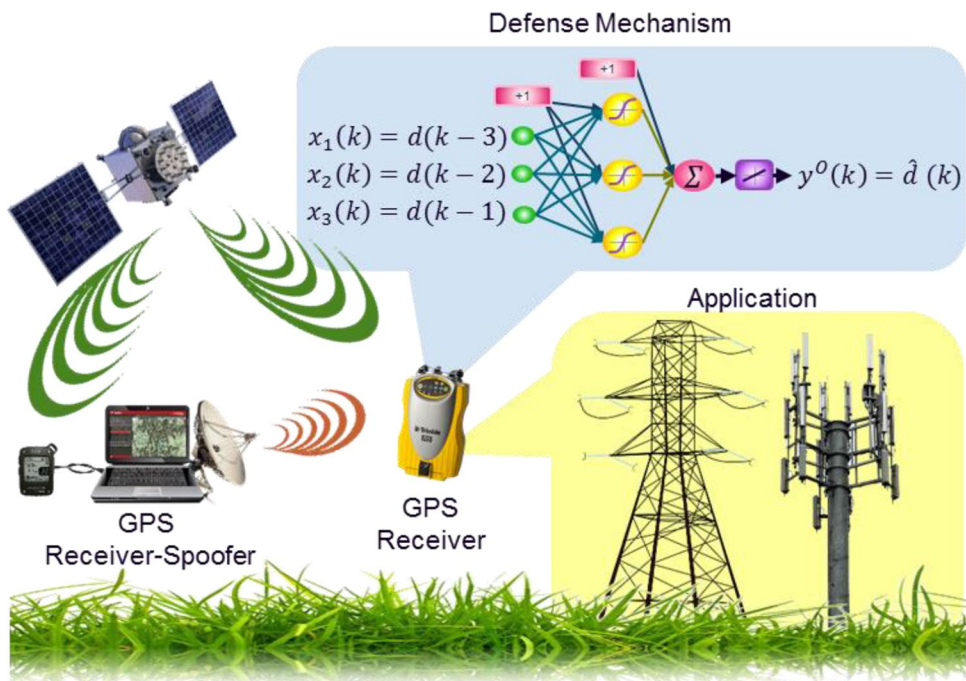


Fig. 3 Performance comparison for different NN structures with sigmoid activation function

Fig. 4 Scheme of TSA on a typical GPS receiver and applying the proposed MLP NN as a defense mechanism is depicted. The proposed MLP NN has three nodes in the input layer, three neurons in the hidden layer, and a single output layer



is the estimation of the clock offset, denoted by $\hat{d}(k)$, at the present time instant k .

According to (22), the network order is 16, which indicates a reasonable amount of complexity. The network has been trained with the Levenberg–Marquardt algorithm, which provides an acceptable response and fast convergence rate (Hagan and Menhaj 1994). A dataset of 200 samples of clock offset is exploited in the learning procedure, representing 200 s of information. The first half of the dataset, collected by Lee et al. (2019), has been exploited for this purpose. They utilized a Google Nexus 9 tablet, which has an embedded GPS chipset, to collect the data on November 4, 2018, at the San Antonio campus of the University of Texas. The complete dataset will be utilized in the following sections to evaluate the proposed network. The training process of the network is conducted by 70% of data, while its performance is validated by 15% of samples. The other 15% of the data is employed to test network efficiency. Furthermore, the dataset is scaled to increase the convergence rate (LeCun et al. 2012). The MSE results of the training process are exhibited in Fig. 5.

The proposed MLP NN has been exploited in an error-based detection algorithm, which can identify the type of TSA. The flowchart of the algorithm is exhibited in Fig. 6. According to the figure, the estimation error of the network is defined as:

$$e_{est}(k) = d(k) - \hat{d}(k) \tag{23}$$

where $d(k)$ is the extracted clock offset information from the navigation solution of the receiver and $\hat{d}(k)$ is the MLP NN estimation of the current sample based on the previous three

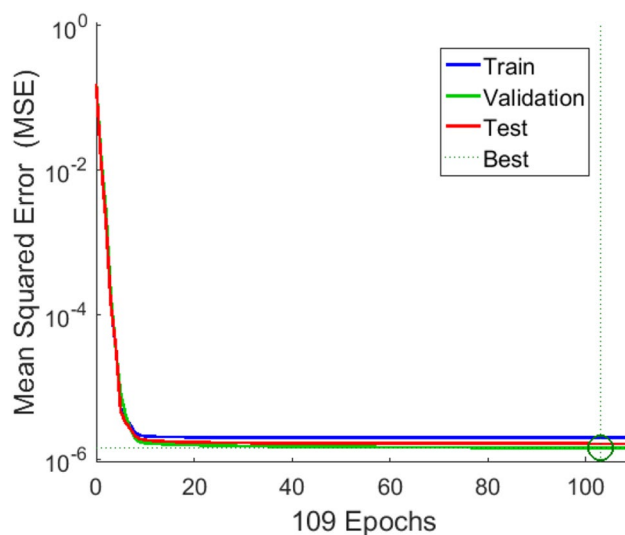
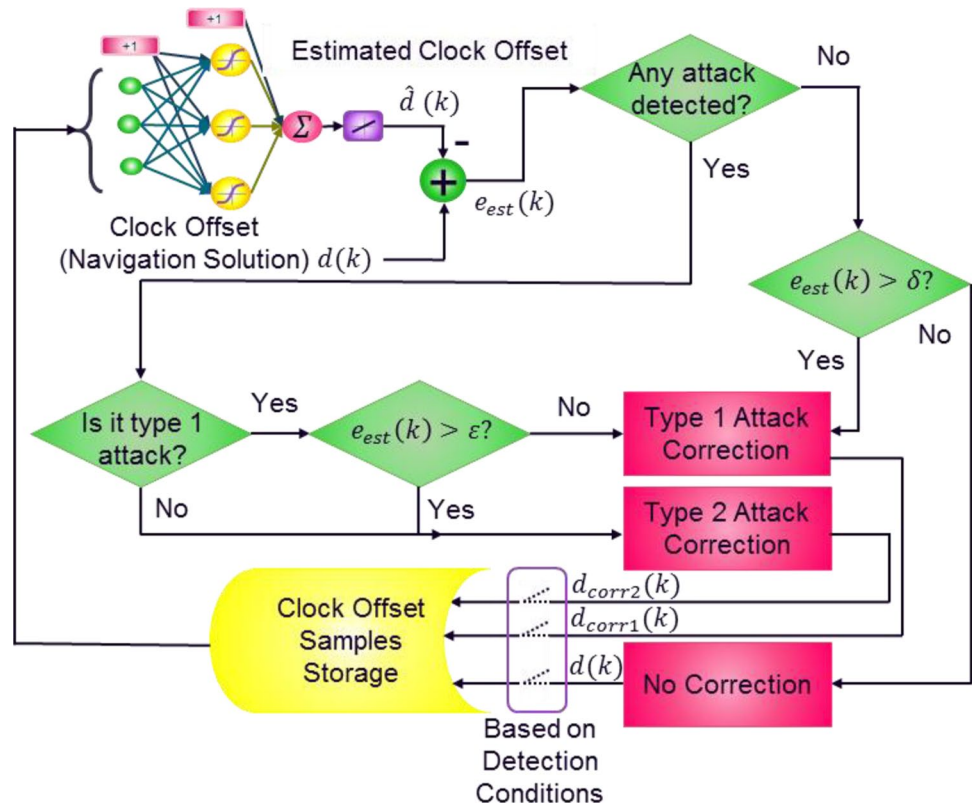


Fig. 5 Learning process of MLP NN and MSE of each iteration with the Levenberg–Marquardt algorithm is exhibited. The best validation performance is 1.4341×10^{-6} at epoch 103

samples. The application and its sensitivity to the clock offset errors determine the threshold of attack detection, which is denoted by δ . Therefore, if the error between the predicted sample and receiver solution is higher than δ ($e_{est}(k) > \delta$), the error will be intolerable for that specific application. The IEEE C37.118 declares that the 1% total variation error is regarded as an intentional attack on PMUs (Martin 2011). The amount is equal to 26.65 μ s of clock offset error or equivalent distance of 7989 m (Lee et al. 2019).

Fig. 6 Estimation error, the difference of MLP NN output and clock offset, through a series of threshold conditions leads to the spoof detection and error mitigation



In the first type of attack, the clock offset error is introduced abruptly into the samples; thus, the $e_{est}(k)$ is increased drastically at once and leads the algorithm to detect the attack. The estimation error is considered a correction coefficient for sample refinement and expresses the amount of the injected clock offset. The second type of attack modifies the clock offset distinctly: The error is added to samples gradually. In the first type of attack, the correction coefficient remains constant, while for the second attack, the value has to be updated in each iteration based on $e_{est}(k)$. The second error threshold ϵ is determined to exhibit the amount of parameter update under the condition of the second type of attack.

Experimental results and performance evaluation

In this section, the performance of the proposed MLP NN is evaluated through two real-world datasets with different characteristics. The first dataset has been provided by the authors of Lee et al. (2019) and is available on the Github Web site. A tablet equipped with a GPS chipset is used to record the first dataset on November 4, 2018, at the University of Texas at the San Antonio main campus, and the GNSS Logger android application (Google 2020) is employed to derive the navigation solution. The dataset

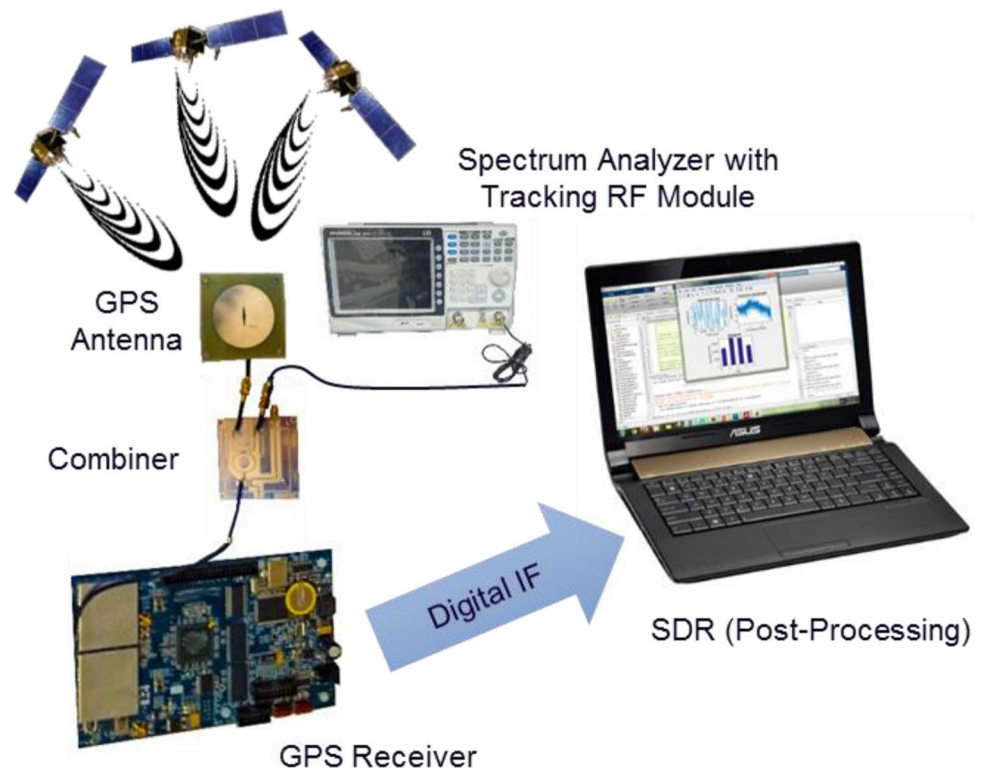
contains 400 samples that are representing 400-s information of a stationary receiver.

A hardware equipment set including a GPS receiver and a spectrum analyzer with a tracking RF module is exploited for retrieving the second dataset, as shown in Fig. 7. The receiver captures the RF signal, combines it with the GPS simulator signal, and passes it through a band-pass filter and amplifier. The signal is downconverted to the IF; then, the results are digitized and stored for further processing. A temperature-compensated crystal oscillator (TCXO) has been utilized as a clock oscillator. A SDR is exploited for the acquisition, tracking, and extraction of the navigation solution. The dataset has been recorded on April 24, 2014, at Valiasr Street, Tehran, Iran, with a sampling frequency equal to 5.7143 MHz. It should be noted that the receiver has been stationary during the data recording procedure. Matlab® R2016a is employed to extract the solution and corresponding clock offset information. The duration of the obtained dataset is 32.5 s, which is expressed by 400 samples. Furthermore, Matlab® is used to train and test the MLP NN. The network has been trained with a unified dataset of 200 samples that has the same characteristics as the first dataset.

TSA configuration and estimation methods

The first type of TSA is configured by a step-shaped signal with an 8000 m offset or time equivalent of $26.68 \mu s$. The

Fig. 7 GPS signal collection. The GPS signals are collected through an antenna, and after passing the RF front end, the digitized samples of the signals are saved for further processing and extracting the PVT solution



attack is abruptly added to the signal at the 30th time sample for the first dataset. The malicious signal is injected into the raw pseudoranges of the second dataset at the 69th sample. A gradually increasing signal is a representative of the spoofing signal in the second attack, which is injected to data at the same time samples, as mentioned for the first type. The disruptive modifications are performed on the raw measurements of all pseudoranges. This type of attack only affects the clock offset information, while the location of the receiver remains constant. Both attacks on datasets remain until the last sample of the data.

TSA are generated in the same way as expressed in the RE work (Lee et al. 2019) for a fair comparison with the proposed MLP NN. Furthermore, the performance of MLP NN is compared with the well-known EKF (Axelrad and Brown 1996) and Luenberger observer (LO) (Luenberger 1966) as classical approaches to estimate the clock offset. Root mean square error (RMSE) is exploited to conduct the assessment of methods and is defined as:

$$RMSE = \sqrt{\frac{1}{N} \sum_{k=1}^N (dt_u(k) - \hat{dt}_u(k))^2} \quad (24)$$

where $dt_u(k)$ is the true value of the clock offset, $\hat{dt}_u(k)$ is the estimated one, and N is the number of samples involved in the assessment.

Evaluation of methods with first dataset

The GPS navigation estimator has to estimate position, clock offset, and clock drift in stationary applications. The navigation algorithm merges the raw measurements of the receiver and the satellite positions to estimate the user state. EKFs are widely exploited in stand-alone systems and linearize the models with the current best estimate of the receiver state (Axelrad and Brown 1996). Moreover, LO is a linear time-invariant system that is able to eliminate the noise disturbances of the measurements (Luenberger 1966). Both EKF and LO are classical methods of receiver state estimation, which are not resistant to any types of spoofing attacks, as shown in Figs. 8 and 9.

According to the top panels of Figs. 8 and 9, the injected modifications of both types of TSA misled EKF and LO. In the first type of attack, a constant amount of error is shown in the bottom panel of Fig. 8 for EKF and LO, which indicates the impact of the step-shaped spoofing signal. Although, the performances of RE and proposed MLP NN are significantly better than classical approaches. The magnified part of the top panel of Fig. 8 indicates a fluctuation in the RE behavior caused by the abrupt injection of the attack signal. However, the MLP NN has not been affected by the sudden introduction of TSA.

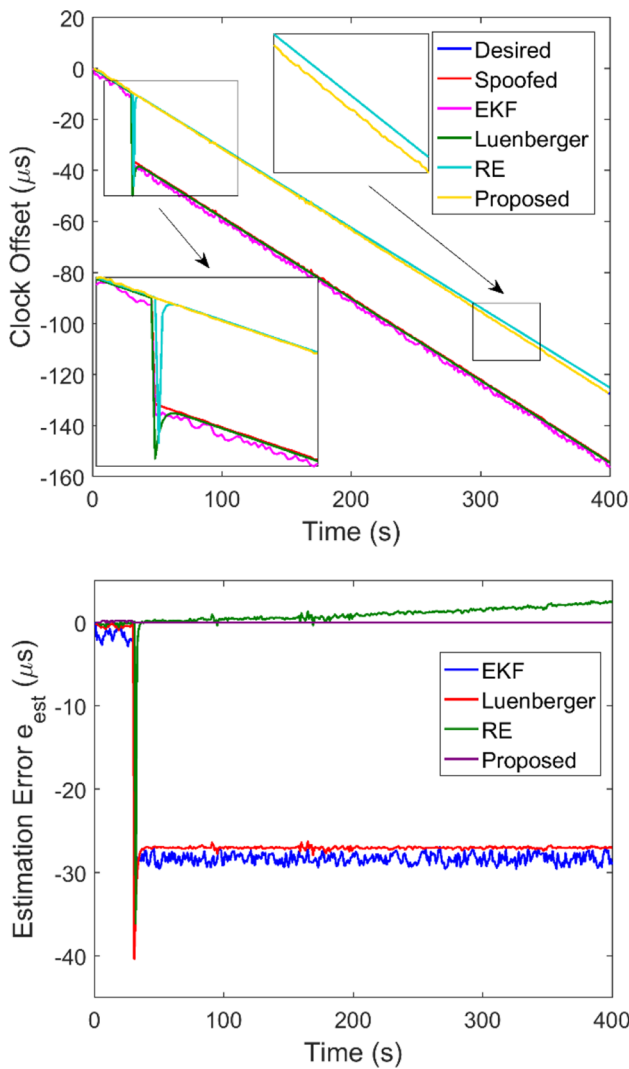


Fig. 8 Evaluations of methods with the first dataset. Clock offset information modifications on the first-type TSA (top), and estimation errors of each method (bottom)

RE relies on the dynamic model for stationary applications under spoofing attacks. The main issue with estimations based on the models of the system is their limited knowledge of the signal, which causes a deterioration in estimation conditions. Regarding the bottom panel of Fig. 8, e_{est} of RE is increasing as time passes, while the proposed method has a stable e_{est} . The reason for MLP NN stability is its knowledge of clock offset trend, which is obtained in the training procedure. The knowledge facilitates maintaining the quality of estimation during the epochs.

The same situation has occurred in the second type of TSA for EKF and LO, and the increasing behavior of TSA caused rising estimation errors, which are exhibited in Fig. 9. Estimations of RE and MLP NN are very close

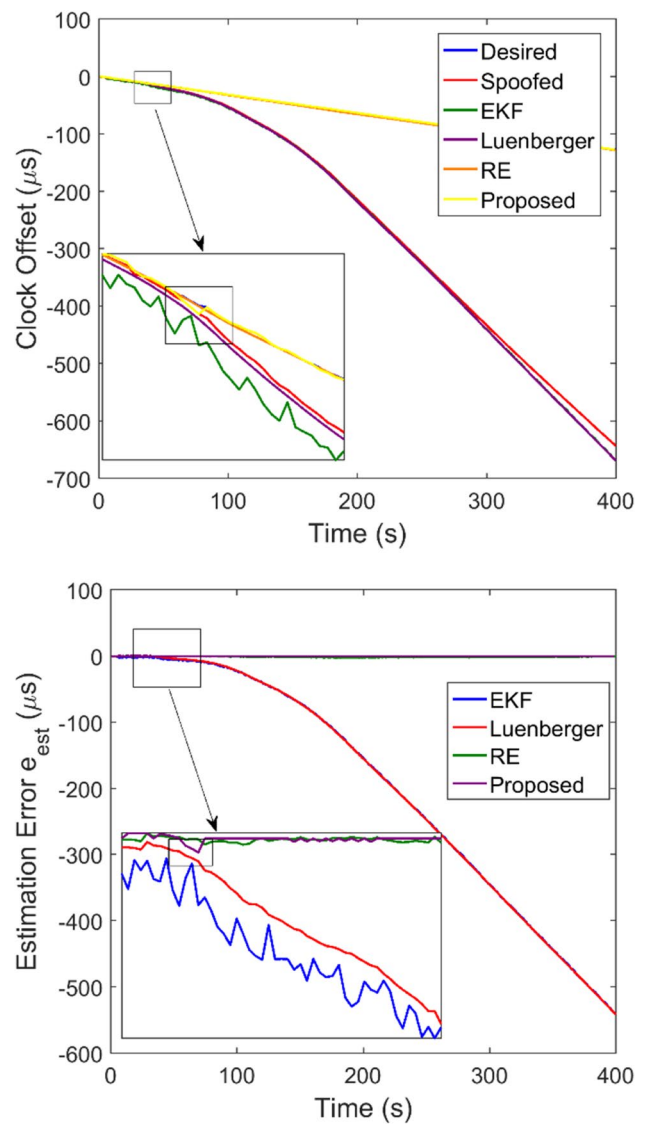


Fig. 9 Evaluations of methods with the first dataset. Clock offset information modifications on the second-type TSA (top), and estimation errors of each method (bottom)

to the true clock offset and indicate their high accuracy based on e_{est} shown in the bottom panel of the figure. The magnified sections of Fig. 9 indicate the mechanism of δ threshold: The difference between the MLP NN estimated value and spoofed one increases until it reaches δ . At this point, the attack is detected, and MLP NN knowledge facilitates omitting the excessive modifications caused by TSA. The RMSE of each method is expressed in Table 1, which confirms the superiority of MLP NN method. It is also worth noting that $\delta = 0.15\mu s$ and $\epsilon = 0.15\mu s$ are exploited in this set of experiments. Thresholds have been chosen based on the range of the input data and its variations for higher precision.

Table 1 MSEs of each method under the TSA conditions for the first dataset (expressed in μs)

TSA type	EKF	LO	RE	Proposed MLP NN
Type 1	27.24	26.05	2.19	0.051
Type 2	261.003	261.37	1.30	0.070

Performance assessment of methods with second dataset

The characteristics of the second dataset are quite different from the first one. The higher data range and an abrupt alteration in the middle of the clock offset samples create challenging conditions for most of the estimation algorithms. The GPS receivers have limited storage space; therefore, they cannot store large clock offsets. According to this point, prescribed ranges are defined for the clock offset. Every time the clock offset exceeds the ranges, the receiver clock is updated to maintain the limits. This update will cause a jump in the clock offset. The attack conditions or other factors can alter the update periods slightly; thus, the clock offset behavior is pseudo-periodic. Due to the weak performance of EKF and LO in the former dataset, only the results of RE and the proposed MLP NN are considered in the second dataset performance evaluation. The TSA modifications on the signal are the same as the previous subsection.

The top panel of Fig. 10 exhibits the response of each method to the first-type TSA. Previously, the RE algorithm reaction to the attack has been manifested as a fluctuation in the estimation. In this dataset, no fluctuations were observed in the behavior of the algorithm, and RE estimated the clock information slightly higher than the desired value. The bottom panel of Fig. 10 indicates a high estimation error for MLP NN at the first samples of data. The network has been trained with a dataset whose initial values are near zero. Therefore, it takes a few samples for the network to adapt to the conditions of the new dataset and emendates the error. Both methods carry a constant error value after attack injection. However, MLP NN attempts to reduce e_{est} with a fluctuation, yet a slight amount of error is not compensated, as shown in the magnified part of the bottom panel of Fig. 10.

The responses of RE and the proposed MLP NN to the second type of attack are depicted in Fig. 11. The reactions to the attack are similar to Fig. 10, with respect to the high e_{est} of the MLP NN at first samples of the dataset. Furthermore, a fluctuation is observed in the estimation error of RE concerning the sudden alteration of the data samples. The correction mechanism based on the ϵ value for the gradually increasing nature of second-type TSA is exhibited in the magnified part of the bottom panel of Fig. 11. Every time the estimation error is higher than ϵ , the algorithm corrects

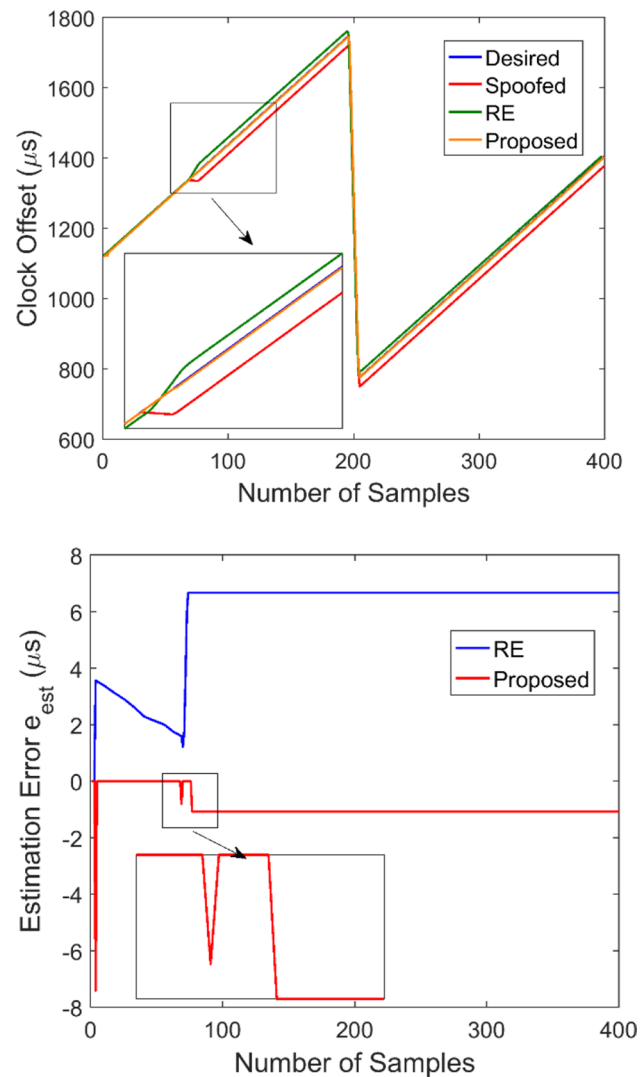


Fig. 10 Performance of RE and the proposed MLP NN with the second dataset. Clock offset information modifications on the first-type TSA (top) and estimation errors of each method (bottom)

the erroneous clock offsets, which causes the sawtooth-shaped e_{est} . The value of ϵ determines the height of each peak: Lower ϵ results in small peaks and contrariwise. The RMSE values for each algorithm alongside the choices for ϵ and δ are presented in Table 2. The premier performance of the proposed MLP NN is established based on better RMSE results.

Discussion on attack detection and corrections for second dataset

The receiver clock update procedure causes a fluctuation in the clock offset trend. This large modification in the smooth trend of the clock offset can be detected as a spoofing attack in some of the monitoring methods. In this subsection, the

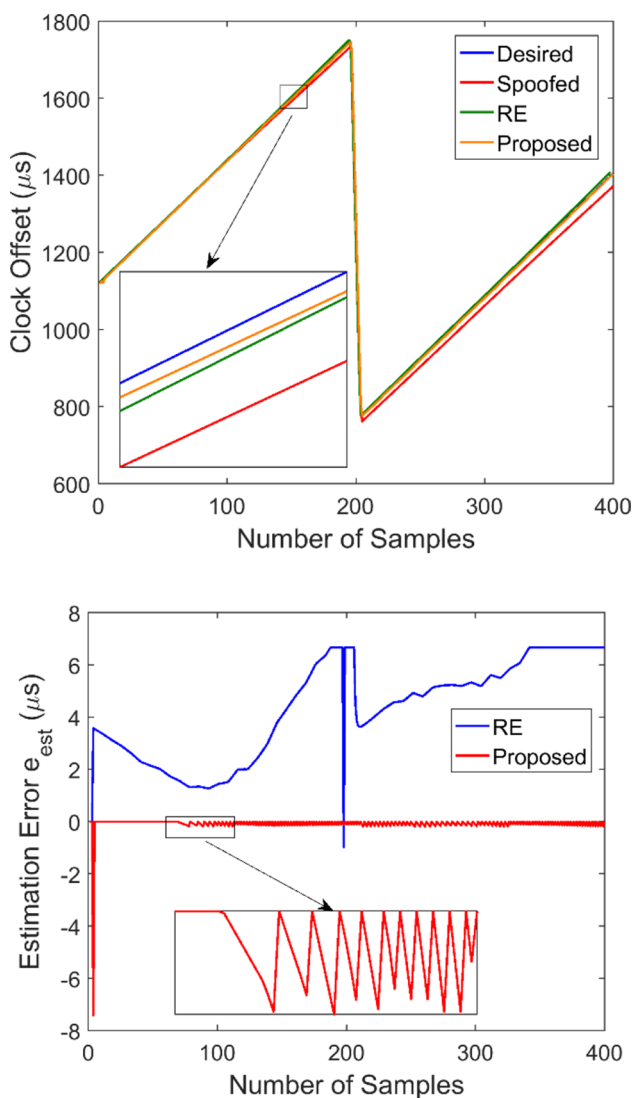


Fig. 11 Performance of RE and the proposed MLP NN with the second dataset. Clock offset information modifications on the second-type TSA (top) and estimation errors of each method (bottom)

Table 2 RMSEs of RE and the proposed MLP NN and correction algorithm parameters for the second dataset (expressed in μs)

TSA type	RE	Proposed MLP NN	δ	ϵ
Type 1	6.16	1.03	4.8	2
Type 2	4.71	0.38	4.8	0.2

response of the proposed method to the fluctuation is investigated, specifically. Hence, an attack-free case is considered to evaluate the performance of the network, and the results are demonstrated in Fig. 12. According to the top panel, both RE and MLP NN have followed the trend with acceptable performance. However, the bottom panel exhibits an

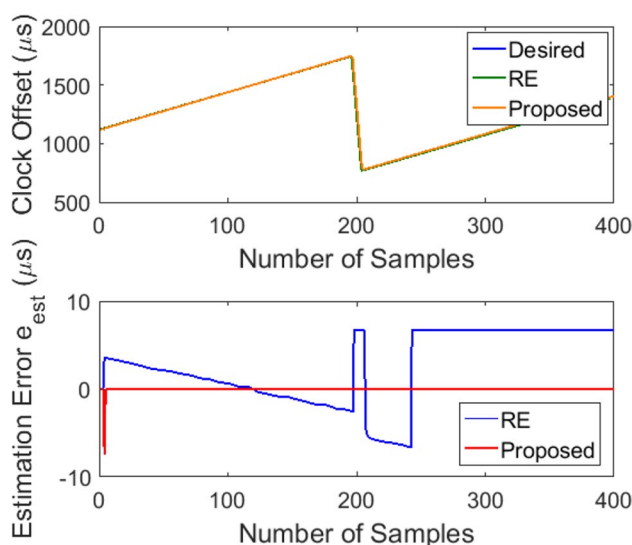


Fig. 12 Estimation errors (bottom) of RE and MLP NN demonstrate the effects of the update fluctuation in the clock offset trend (top) for the attack-free case

increase in e_{est} of RE, which has subsided after a short while. The fluctuation affects the performance of RE, and another raise is observed after the 250th sample. Furthermore, the bottom panel of Fig. 11 exhibits the same behavior for RE. On the other hand, the fluctuation has not affected the e_{est} of MLP NN, and the value remains the same. As noted earlier, an error of $26.65 \mu s$ is considered a spoofing attack (Lee et al. 2019). The effect of the fluctuation on the RE method introduced an error of less than ten microseconds; thus, the resultant error does not trigger any false alarms.

According to Fig. 6, the proposed method exploits two thresholds, δ and ϵ . Any estimation error higher than δ arises speculations of a spoofing attack occurrence; thus, the algorithm starts to correct the clock offsets based on the network knowledge. At this time, if the introduced e_{est} rises higher than $26.65 \mu s$ and remains high for a few samples, then speculations about the first type of attack turn to assurance. On the other hand, if the error does not exceed the threshold, the algorithm keeps observing e_{est} and updates the correction coefficient using ϵ . Similar to the first type of attack detection, when the correction coefficient passes the attack threshold for a few samples, it can be stated that the second type of attack is detected. Any time that the coefficient exceeds the predetermined value ($26.65 \mu s$), the attack is detected. Attack-free, the first type, and the second type of attack are depicted in the top, middle, and bottom panels of Fig. 13, which are associated with the second dataset.

Values of δ and ϵ affect the RMSE, as shown in Fig. 14. The best results of the network are obtained with $\delta \in (0, 5 \mu s]$ and $\epsilon \in (0, 3 \mu s]$. According to the figure, a value near $5 \mu s$ is suitable for δ , since it provides the lowest possible RMSE

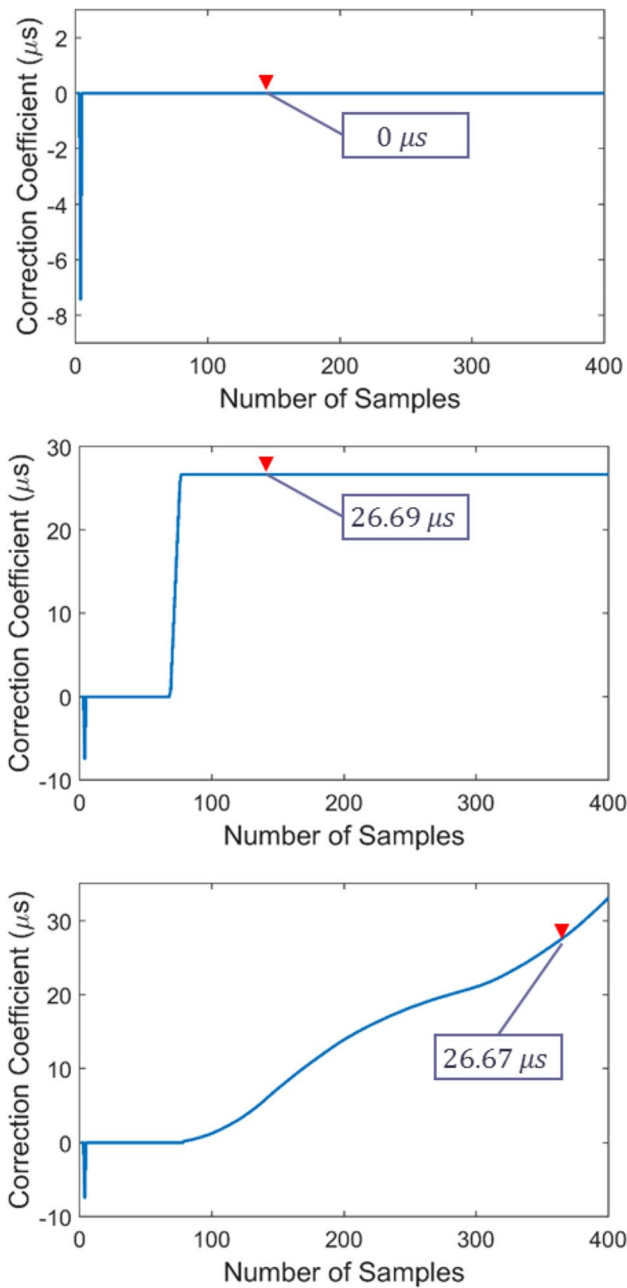


Fig. 13 Correction coefficients of the attack-free case are demonstrated on the top panel. The middle and bottom panels represent the same values for the first and second types of attack

and the highest speculation limit. The second coefficient, ϵ , has a selection range of $(0, 3 \mu\text{s}]$, in which the higher values lead to fewer corrections, and lower ones update the correction coefficients at a faster pace. Therefore, it is suggested to select the lower values for ϵ in case of unknown behaviors such as a second-type attack. High uncorrected estimation errors cause a gap between the authentic trend and the estimated one, which increases the RMSE, as shown in the yellow region of Fig. 14.

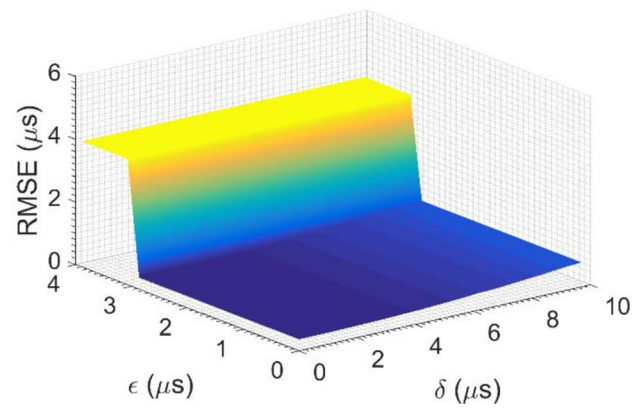


Fig. 14 RMSE of the proposed method is depicted as a function of δ and ϵ thresholds

Discussion and conclusion

An MLP NN is contributed in this research to address the security issues concerning the clock offset information of a stationary receiver. Two datasets with different features have been exploited to evaluate the performance of the proposed method. The first dataset has straightforward features, while the second one is more challenging for most of the estimators. GPS signals of the second dataset are gathered through a GPS receiver, and the digitized signal samples are stored in a computer to extract the navigation solution. Due to the pseudo-periodic receiver clock updates, the behavior of the clock offset over time does not change drastically, and the proposed MLP NN has the same long-time performance.

Two well-known types of TSA are applied to the raw measurements of pseudorange in each dataset. The performance of the proposed method is compared to the EKF, LO, and RE, and the achieved RMSEs of the proposed method are at least six times better than the state-of-art RE. The security-sensitive applications such as PMUs and communication towers can exploit the proposed MLP NN as well as other applications that require precise timing information. Additionally, the utilization of the method does not demand extra hardware or software resources, and firmware update of the GPS receiver can fortify it against a vast number of TSAs or other error sources.

Data availability The first dataset belongs to Lee et al. (2019) and is available at <https://github.com/junhwanlee95/Robust-Estimator>. The second dataset that verifies the findings of this study is available from the corresponding author upon reasonable request.

References

3GPP2 (2004) Recommended minimum performance standards for cdma2000 spread spectrum base stations

- Axelrad P, Brown RG (1996) GPS navigation algorithms. Global positioning system: theory and applications, vol I. American Institute of Aeronautics and Astronautics, Washington, pp 409–433
- Bhamidipati S, Kim KJ, Sun H, Orlik PV (2019) Wide-area GPS time monitoring against spoofing using belief propagation. In 16th annual IEEE international conference on sensing, communication, and networking (SECON). IEEE, pp 1–8
- Bonebrake C, O'Neil RL (2014) Attacks on GPS time reliability. *IEEE Secur Priv* 12(3):82–84
- Borre K, Akos DM, Bertelsen N, Rinder P, Jensen SH (2007) A software-defined GPS and Galileo receiver, a single frequency approach. Springer, Birkhauser Boston
- Diggelen F, Enge P, (2015) The world's first GPS MOOC and worldwide laboratory using smartphones. In Proceedings of the 28th international technical meeting of the satellite division of the institute of navigation (ION GNSS+ 2015), pp 361–369
- Fan X, Du L, Duan D (2018a) Synchronphasor data correction under GPS spoofing attack: a state estimation-based approach. *IEEE Trans Smart Grid* 9(5):4538–4546
- Fan X, Pal S, Duan D, Du L (2018) Closed-form solution for synchronphasor data correction under GPS spoofing attack. In IEEE Power & Energy Society General Meeting (PESGM). IEEE, pp 1–5
- Ghorbani K, Orouji N, Mosavi MR (2020) Navigation message authentication based on one-way hash chain to mitigate spoofing attacks for GPS L1. *Wireless Pers Commun* 113(4):1743–1754
- Google (2020) Raw GNSS measurements. <https://developer.android.com/guide/topics/sensors/gnss>. Accessed 2020
- Hagan MT, Menhaj MB (1994) Training feedforward networks with the Marquardt algorithm. *IEEE Trans Neural Networks* 5(6):989–993
- Haykin SO (2009) *Neural networks and learning machines*, 3rd edn. Pearson, London
- Heng L, Chou D, Gao GX (2014) Reliable GPS-based timing for power systems: a multi-layered multi-receiver architecture. *Inside GNSS*, November/December 2014
- Jiang X, Zhang J, Harding BJ, Makela JJ, Dominguez-Garcia AD (2013) Spoofing GPS receiver clock offset of phasor measurement units. *IEEE Trans Power Syst* 28(3):3253–3262
- Karim R (2019) Counting No. of parameters in deep learning models. Towards data science. <https://towardsdatascience.com/counting-no-of-parameters-in-deep-learning-models-by-hand-8f1716241889>. Accessed 2019.
- Khalajmehrabadi A, Gatsis N, Akopian D (2018a) Evaluation of the detection and mitigation of time synchronization attacks on the global positioning system. In 2018 IEEE/ION Position, Location and Navigation Symposium (PLANS). IEEE, pp 1368–1371
- Khalajmehrabadi A, Gatsis N, Akopian D, Taha AF (2018) Real-time rejection and mitigation of time synchronization attacks on the global positioning system. *IEEE Trans Industr Electron* 65(8):6425–6435
- LeCun YA, Bottou L, Orr GB, Müller KR (2012) Efficient BackProp. In: Montavon G, Orr GB, Müller KR (eds) *Neural networks: tricks of the trade*. Springer, Berlin, pp 9–48
- Lee J, Taha AF, Gatsis N, Akopian D (2019) Tuning-free, low memory robust estimator to mitigate GPS spoofing attacks. *IEEE Control Systems Letters* 4(1):145–150
- Lewandowski W, Petit G, Thomas C (1993) Precision and accuracy of GPS time transfer. *IEEE Trans Instrum Meas* 42(2):474–479
- Li X, Ge M, Dai X, Ren X, Fritsche M, Wickert J, Schuh H (2015) Accuracy and reliability of multi-GNSS real-time precise positioning: GPS, GLONASS, BeiDou, and Galileo. *J Geodesy* 89(6):607–635
- Luenberger D (1966) Observers for multivariable systems. *IEEE Trans Autom Control* 11(2):190–197
- Magiera J (2019) A multi-antenna scheme for early Detection and mitigation of intermediate GNSS spoofing. *Sensors* 19(10):2411
- Martin KE (2011) Synchronphasor standards development - IEEE C37.118. In 2011 44th Hawaii international conference on system sciences. IEEE, pp 1–8
- Mosavi MR (2006) Comparing DGPS corrections prediction using neural network, fuzzy neural network, and Kalman filter. *GPS Solut* 10(2):97–107
- Mosavi MR, Baziar AR, Moazedi M (2017) De-noising and spoofing extraction from position solution using wavelet transform on stationary single-frequency GPS receiver in immediate detection condition. *J Appl Res Technol* 15(4):402–411
- Mosavi MR, Shafiee F (2016) Narrowband interference suppression for GPS navigation using neural networks. *GPS Solutions* 20(3):341–351
- Mosavi MR, Tabatabaei A, Zandi MJ (2016) Positioning improvement by combining GPS and GLONASS based on Kalman filter and its application in GPS spoofing situations. *Gyroscop Navig* 7(4):318–325
- Musleh AS, Chen G, Dong ZY (2019) A survey on the detection algorithms for false data injection attacks in smart grids. *IEEE Transactions on Smart Grid* 11(3):2218–2234
- Psiaki ML, O'Hanlon BW, Bhatti JA, Shepard DP, Humphreys TE (2013) GPS spoofing detection via dual-receiver correlation of military signals. *IEEE Trans Aerosp Electron Syst* 49(4):2250–2267
- Riedel C, Fu G, Beyette D, Liu JC (2019) Measurement system timing integrity in the presence of faults and malicious attacks. In: Paper presented at international conference on smart grid synchronized measurements and analytics (SGSMA). IEEE, pp 1–8.
- Schmidt D, Radke K, Camtepe S, Foo E, Ren M (2016) A Survey and analysis of the GNSS spoofing threat and countermeasures. *ACM Comput Surv* 48(4):1–31
- Schmidt E, Lee J, Gatsis N, Akopian D (2020) Rejection of smooth GPS time synchronization attacks via sparse techniques. *IEEE Sens J* 21(1):776–789
- Schmidt E, Ruble Z, Akopian D, Pack DJ (2019) Software-defined radio GNSS instrumentation for spoofing mitigation: a review and a case study. *IEEE Trans Instrum Meas* 68(8):2768–2784
- Shafiee E, Mosavi MR, Moazedi M (2018) Detection of spoofing attack using machine learning based on multi-layer neural network in single-frequency GPS receivers. *J Navig* 71(1):169–188
- Shepard DP, Humphreys TE, Fansler AA (2012) Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks. *Int J Crit Infrastruct Prot* 5(3–4):146–153
- Siamak S, Dehghani M, Mohammadi M (2020) Dynamic GPS spoofing attack detection, localization, and measurement correction exploiting PMU and SCADA. *IEEE Syst J*. <https://doi.org/10.1109/JSYST.2020.3001016>
- Wang Y, Chakraborty A (2016) Distributed monitoring of wide-area oscillations in the presence of GPS spoofing attacks. In 2016 IEEE power and energy society general meeting (PESGM). IEEE, pp 1–5.
- Xie J, Meliopoulos APS (2020) Sensitive detection of GPS spoofing attack in phasor measurement units via quasi-dynamic state estimation. *Computer* 53(5):63–72
- Zhang Z, Zhan X (2016) GNSS spoofing network monitoring based on differential pseudorange. *Sensors* 16(10):1771
- Zhu F, Youssef A, Hamouda W (2016) Detection techniques for data-level spoofing in GPS-based Phasor measurement units. In: Paper presented at 2016 international conference on selected topics in mobile & wireless networking (MoWNeT). IEEE, pp 1–8



N. Orouji received her B.S. degree in Electronic Engineering from K.N. Toosi University of Technology, Tehran, Iran, in 2014, and her M.S. degree in Digital Electronic Systems from Iran University of Science and Technology, Tehran, Iran, in 2017. She is currently a Ph.D. candidate in Electronic Engineering at Iran University of Science and Technology. Her research interests are specialized architecture design, system security, and novel co-processors.



M. R. Mosavi received his B.S., M.S., 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 400 scientific publications in journals and international conferences in addition to 11 *academic* books. His research interests include circuits and systems design.