Spoofing Mitigation of GPS Receiver using Least Mean Squares-Based Adaptive Filter

M. R. Mosavi*(C.A.) and Z. Shokhmzan*

Abstract: The Global Positioning System (GPS) signals are very weak signal over wireless channels, so they are vulnerable to in-band interferences. Therefore, even a low-power interference can easily spoof GPS receivers. Among the variety of GPS signal interference, spoofing is considered as the most dangerous intentional interference. The spoofing effects can mitigate with an appropriate strategy in the receiver. In this paper, we use methods of adaptive filter based on Least Mean Squares (LMS) and Normalized Least Mean Squares (NLMS) algorithms in order to defense against spoofing. The new approaches based on LMS and NLMS are applied in the acquisition stage of the receiver. The new approaches are operated to mitigate effect of spoofing from the received signal in GPS valid receiver. LMS-based algorithm is a class of adaptive filter that modify the filter coefficients to minimize the error signal. NLMS algorithm is a modified form of the normal LMS algorithm that solves the LMS problem by normalizing with the power of the input signal. The proposed methods have been implemented on real dataset. The results explain that the suggested algorithms significantly decrease spoofing. Also, they improve Position Dilution of Precision (PDOP) parameter. Based on the results, NLMS algorithm has better performance than LMS algorithm.

Keywords: Adaptive Filter, GPS, LMS, Mitigation, NLMS, PDOP, Spoofing.

1 Introduction

GPS is a constellation of 32 orbiting satellites which is used for navigation and position measurements [1]. GPS satellites broadcast radio signals over wireless channels to enable GPS receivers on the earth that calculate the exact location, speed and time in all of weather situations. GPS has three parts. The space part contains the collection of orbiting satellites. The user part consists of receivers, which can be accessed by everyone. The control part contains of six ground stations that insure the satellites are working correctly. The GPS system is applied for both civilian and military applications. The GPS is easily accessible to anyone and everywhere with a GPS receiver [2, 3]. The GPS comprises two types of Pseudo Random Noise (PRN) code Coarse/Acquisition (C/A) and Precision (P) code. The C/A code is used by civilian receivers and is easily attainable to the community and the controlled Precision (P) code commonly used for military applications [4]. In this study, we consider civilian receivers and review only the C/A code. All of the satellite signals are modulated onto the same L1 carrier frequency [5]. Each GPS satellite sends data on L1 frequency (1575.42 MHz). The C/A code modulates the L1 carrier [6]. It repeats every 1023 bits with a period of one millisecond and modulates at 1.023 megabits per second (Mbit/s). These sequences only match up, or strongly correlate, when they are exactly aligned. Each satellite has a unique PRN code. Every PRN code does not correlate with any other satellite's PRN code. In other words, the PRN codes are greatly orthogonal to each other. This is a form of Code Division Multiple Access (CDMA), which permits the receiver to identify multiple satellites on the same frequency [7]. In addition to the PRN ranging codes, a receiver needs to know detailed information about each satellite's position.

The navigation message is a low frequency signal added to the L1 codes that gives information about the satellite's orbits, their clock corrections. The navigation message is made up of three parts. The first part contains the GPS date and time, plus the satellite's status and an indication of its health. The second part contains orbital information called ephemeris data and allows the receiver to calculate the position of the satellite. The third part, called the almanac, contains information and status concerning all the satellites; their locations and PRN numbers [8].

Iranian Journal of Electrical & Electronic Engineering, 2015.
Paper first received 23 Feb. 2015 and in revised form 01 Aug. 2015.
* The Authors are with the Department of Electrical Engineering, Iran University of Science and Technology, Tehran, Iran.
E-mails: M_Mosavi@iust.ac.ir, z_shokhmzan@elec.iust.ac.ir.

GPS signals are very weak over wireless channels, so they are in danger to in-band interferences. So, a low-power interference such as blocking, jamming, and spoofing can simply deceive GPS receivers. The goal of such interferences is either to prevent a position lock (blocking and jamming), or to feed the receiver false information so that it computes an erroneous time or location (spoofing). GPS receivers are generally aware of when blocking or jamming is occurring because they have a loss of signal. This spoofing interference is more perilous than jamming because it is surreptitious [9]. The spoofing effects can decrease with an appropriate strategy in the receiver. The structure of spoofing signal is very similar to the satellite signal. Spoofing in its simpler type may refuse navigation by saturating the navigation receiver with authentic, but counterfeit signal. Spoofing is clandestine; so, it is very tasteful attack than both blocking and jamming [10].

Adaptive filtering is a wide area of researcher in the field of communication. Adaptive filters are a class of filters that iteratively alter their parameters in order to minimize a function of the difference between a desired target output and their output. Adaptive noise cancellation is too an approach used for noise reduction in speech signal. As received signal is continuously corrupted by noise where both received signal and noise signal both changes continuously, then this arise the need of adaptive filtering [11].

Acoustic echo occurs when an audio signal is reverberated in a real environment, resulting in the original intended signal plus attenuated, time delayed images of this signal. In the case of acoustic echo cancellation, the optimal output of the adaptive filter is equal in value to the unwanted echoed signal. When the adaptive filter output is equal to desired signal, the error signal goes to zero. In this situation, the echoed signal would be completely cancelled [12].

Spoofing distorts the C/A-code modulations. This makes that the fake satellites participate in the process of navigation solution. Therefore, defense against spoofing attack on GPS receivers has been considered as a serious issue to safety of GPS applications [13]. Appropriate mechanisms are employed for spoofing mitigation in the receiver. This paper presents two approaches based on adaptive filter in both Least Mean Squares (LMS) and Normalized Least Mean Squares (NLMS) algorithms to reduce the spoofing effect on GPS signals.

The remaining part of this paper is organized as follows. Section 2 introduces a brief discussion on different methods of defense against spoofing. Analysis of GPS spoofing signals are described in section 3. In section 4, new approaches for spoofing mitigation in GPS receiver present and the filter weights are calculated using LMS or NLMS algorithms. Section 5 discusses the experimental results on the measured dataset. Then, concluding remarks are given in section 6.

2 Related Works

Several techniques for defense against spoofing which have been presented in the papers are as follows. Vestigial Signal Defense (VSD) is a technique for spoofing detection on the GPS signal [8]. The VSD consists of distinguishing the vestige of the authentic signal and separating it from a multi-path signal that only can be done if the authentic signal has not been merged by the spoofer. To determine the vestigial genuine signal, the target receiver employs the software-defined model. First, the receiver copies the received front-end signal into a buffer applied only for vestigial identification. Then, the receiver chooses one of the GPS signals being tracked and takes away this signal from the buffer. This is the alike way applied to remove strong signals in battling the near/far problem in spread spectrum multiple access systems, containing GPS [14].

The multi-antenna defense seems one of the strongest non-cryptographic defense, which supervises differential carrier phase to detect GPS signals that originates from a point source as opposed to multiple GPS satellites. The defense needs a space of two or more antennas that supplied by a considerable amount of the almost 20 cm GPS signal wavelength. This enhances receiver costs, weight and size. Thus the multi-antenna defense is not widely used by commercial GPS companies [15]. Shepard [16] determined which the correlation peak interplay between the original signal and the interference signal is very like to line of sight and multi-path interplay. Thus, methods of multi-path detection and reduction can be used this type of interference. Signal Quality Monitoring (SQM) is the method for multi-path discovery that identifies interference on the tracking receiver [17]. Ledvina et al (2010) used the delta and ratio SQM tests for interference discovery [18].

Afterwards, Ledvina employed an algorithm of Receiver Autonomous Integrity Monitoring (RAIM) to identify and reduce interference in position and navigation issues [19]. This approach via statistical hypothesis testing detects pseudo-range measurement error and this error is removed from the navigation solution [20, 21].

Cryptographic techniques enable the receiver to detect valid signals from interference signals with high probability [22]. In 2003, Logan Scott presented a cryptographic anti-spoofing technique according to Spread Spectrum Security Codes (SSSC) [23]. The presentment of the SSSCs has insignificant effect on receivers, since L1C acquisition and tracking happens on the pilot channel. In the same reference, Scott also offered Navigation Message Authentication (NMA) method [24]. If SSSC implementation on L1C is impractical, the method of NMA provides a strong renewed selection. The NMA method inserts public-key digital signatures in the resilient Civil Navigation (CNAV) message structure that provides a suitable transition for such signatures [25, 26].

3 Investigation of GPS and Spoofing Signals

We firstly present GPS authentic signal transmitted from satellite. It follows that the signal transferred from satellite k can be defined as:

$$x_{Ak}(t) = \sqrt{2Pc}\left(C_k(t) \oplus D_k(t)\right)\cos(2\pi f_{L1} t) + N_k \quad (1)$$

where P_C is the power of signal, C_k is the C/A code apportioned to satellite number k, D_k is the navigation data, and f_{L1} is the carrier frequency of L1. N_k is a sequence of independent and identically distributed zero mean Gaussian noise samples with variance σ^2 that imitates the effects of thermal noise in the RF front-end [25].

We now explain type of GPS spoofing attack and investigate how our attacker can mislead the locations of GPS receivers. A counterfeit receiver delays authentic signal to produce spoofing signals. Since power of the spoofing signal to be larger than the valid signal, it is increased by a constant greater than one. Then combining of the delayed and valid signal arrive the GPS receiver. Actually, the received signal is sum of the valid and spoofing signal in the genuine receiver [26]. As a result, two alike signals are received only by a single-frequency GPS receiver, however one of signals is delayed. The Eq. (2) demonstrations the spoofed signal in the counterfeit receiver after spoofing.

$$x_{sk}(n) = a x_{Ak}(n - d) \quad (2)$$

In this equation, $x_{SK}(n)$ is the spoofed discrete signal, d is known as delay in the deceived signal and $x_{AK}(n)$ is the valid discrete signal. The coefficient $\alpha > 1$ is the spoofed signal's amplitude benefit factor [25].

The combining of valid digital signal with spoofed digital signal is received at a single-frequency valid receiver. This combined signal is known as the spoofing attack that is determined by the discrete signal $x_{Tk}(n)$ in the Eq. (3). So, the digital signal $x_{Tk}(n)$ is an interference signal which has been combined by spoofed and valid signal.

$$x_{Tk}(n) = x_{AK}(n) + x_{sk}(n) \quad (3)$$

4 Strategy of Adaptive Filter for Spoofing Mitigation

As we know, the GPS signal may be disturbed by the spoofer and the unreal and fake signal to reach the receiver. Therefore, it is difficult for the receiver to discovery their valid position. As previously noted, the Eq. (3) shows the spoofing attack in the target receiver. In this section, the new approaches are offered based on the adaptive filters.

Since the GPS spoofing signals are changing continuously, the weights of filter must be updated in real-time to track the authentic signals and suppress the spoofing. So, the adaptive filters than the conventional non-adaptive filters must be selected for spoofing reduction [27]. These methods attempt to mitigate the effect of the spoofing attack in the GPS received signal. According to the discussed cases, the schematic of GPS receiver units and place of spoofing reduction algorithm are presented in Fig. 1.

An adaptive filter is a system with a linear filter that has a transfer function controlled by variable parameters and a means to adjust those parameters according to an optimization algorithm. Adaptive filters are required for some applications because some parameters of the desired processing operation are unknown in advance or are changing. The closed loop adaptive filter uses feedback in the form of an error signal to refine its transfer function. In general, this adaptive process involves the use of a cost function that is a criterion for improving the efficiency of the filter, to satisfy an algorithm [28]. Also, the cost function determines how to adapt filter transfer function to reduce the cost on the next iteration. The mean square of the error signal is often used as the cost function. An adaptive filter is adjusted until the error is minimized. There are two input signals to the adaptive filter, d and x that are occasionally named the primary and the reference input, respectively. Fig. 2 displays the schematic view of adaptive filter which is used in this research.

In this study, the adaptive filter is operated to mitigate effect of spoofing from the received signal in GPS receiver. As considered in section 3, the Eq. (3) is shown as a received signal with spoofing in the GPS receiver. So, signal $x_{TK}(n)$ in the Eq. (3) is employed as a reference signal of an adaptive filter. Both signals d and x contain the GPS valid signal plus spoofing signal that are shown according to the Eq. (4) and the Eq. (5), respectively.

$$d(n) = x'_{AK}(n) + x'_{sk}(n) \quad (4)$$

$$x(n) = x_{Tk}(n) \quad (5)$$

where $x'_{AK}(n)$ and $x'_{SK}(n)$ have similar significations as $x_{AK}(n)$ and $x_{SK}(n)$ in the Eq. (3). $x'_{AK}(n)$ and $x_{AK}(n)$ are valid discrete signals in two neighbor times. $x'_{SK}(n)$ and $x_{SK}(n)$ are too spoofing discrete signals that are transferred by spoofer in two near times. Thus, by using the GPS received signals of two neighbor times as inputs to an adaptive filter, the effects of spoofing can reduce in the receiver. In order to reduce the effects of spoofing attack by the adaptive filters, $x'_{AK}(n)$, $x_{AK}(n)$ and $x_{SK}(n)$ have to establish the following cases [29]:

Fig. 1 Schematic of GPS receiver units and place of spoofing reduction algorithm.

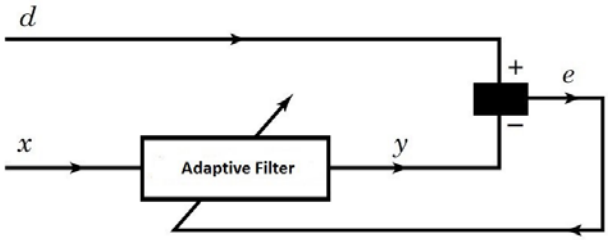

Fig. 2 Schematic view of adaptive filter used in this research.

$$E\left[x'_{Ak}(n)x_{Sk}(n-m)\right]=0 \quad (6)$$

$$E\left[x'_{Ak}(n)x'_{Sk}(n-m)\right]=0 \quad (7)$$

$$E\left[x_{Ak}(n)x'_{Ak}(n-m)\right]=p(m) \quad (8)$$

where *p(m)* is an unknown cross-correlation for lag *m*. $x'_{AK}(n)$ and $x_{AK}(n)$ are extremely correlated. But $x'_{SK}(n)$ and $x_{SK}(n)$ are uncorrelated, which indicates that Eq. (6) and Eq. (7) are partially fulfilled.

4.1 Spoofing Mitigation using LMS Algorithm

The LMS, NLMS and Recursive Least Squares (RLS)-based algorithms are popular types of adaptive filter. In this study, we applied LMS and NLMS-based algorithms to mitigate the effect of spoofing signal in GPS receiver. LMS-based algorithm is a class of adaptive filter that modify the filter coefficients to minimize the error signal. It is an accidental gradient descent technique, which is adjusted based on the error at the present time. Compared to RLS-based algorithms, the LMS-based algorithms do not involve any matrix operations. Therefore, the LMS-based algorithms require fewer computational resources and memory than the RLS algorithms. The implementation of the LMS-based algorithms also is less complicated than the RLS algorithms [28].

The LMS-based algorithm applies the following steps to update the adaptive filter coefficients: a filtering method produce an output in response to an input sequence *x(n),* which have the discrete sample size N. According to Eq. (9), the output signal y(n) is computed from the adaptive filter.

$$y(n)=\sum_{m=0}^{L-1} w_m(n)x(n-m) \quad (9)$$

where L is the length of the adaptive FIR filter. $w_m(n)$ is the filter coefficients and indicates a time-varying transfer function that will be modified based on signal conditions. From Eq. (4) and Eq. (9), the error signal *e*(*n*) is calculated by using the Eq. (10):

$$e(n)=d(n)-y(n)=x'_{Ak}(n)+x'_{sk}(n)-y(n) \quad (10)$$

The filter coefficients are updated by using the following equation:

$$w_m(n+1)=w_m(n)+\mu e(n)x(n-m) \quad m=0,1,...L-1 \quad (11)$$

where μ is the step size of the adaptive filter. This parameter controls how the algorithm converges to the desirable filter coefficients. If step size is very large, the algorithm will diverge. If it is very small the algorithm converges gradually and could not be able to follow altering situations. Therefore, the value of μ satisfies the following range.

$$0<\mu<\frac{2}{\lambda\max} \quad (12)$$

where λ_{max} is the most eigenvalue of the matrix $R = E\{x(n)\, x^H(n)\}$. If this situation is not performed, the algorithm becomes fickle. In order to achieve the optimum weights of adaptive filter, the cost function is minimized. The Mean Square Error (MSE) is used as the cost function that can be expressed as:

$$MSE=E\left\{e^2(n)\right\}=\sum_{n=0}^{N-1} e^2(n) \quad (13)$$

where E means the expectation operator.

4.2 Spoofing Mitigation using NLMS Algorithm

In the LMS algorithm, the modification useable to the weights is straight relative to the input, x(n). Therefore, when x(n) is large, the LMS filters allow to a noise enlargement difficulty. To conquer this problem, the NLMS filter can be operated. NLMS algorithm is a modified form of the normal LMS algorithm. The coefficients of NLMS algorithm are calculated by using the Eq. (14):

$$w_m(n+1)=w_m(n)+\frac{\mu}{\|x(n)\|^2}e(n)x(n-m) \quad m=0,1,...L-1 \quad (14)$$

where $||x(n)||^2$ is the power of input $x(n)$. The NLMS algorithm solves the LMS problem by normalizing with the power of the input [28]. In this algorithm, d and x in the Eqs. (4) and (5) are two inputs for adaptive filter such as LMS algorithm.

In the section 3, we noted that the coefficient α is the delayed signal's amplitude advantage factor. Since the spoofing signal power is more than the authentic signal power, α must be a factor greater than one. Thus in this study α is considered value of 2. In both methods, we employed the adaptive filter with length of 8 and the step size of μ = 0.0003. Note that the methods are applied to the digital IF signal at the acquisition stage in the receiver. The signal of adaptive filter output is arrived to different sections of GPS receiver including the acquisition and tracking. We used the MATLAB software for the simulation. Several dataset was investigated and all results reduced the effect of interference in the receiver. After the navigation solution processing, PDOP parameter is significantly reduced and improved which is the second result achieved in this work.

5 Experimental Results

In this section, we discuss the simulation analysis. The results of new approaches using LMS and NLMS are reported and the first method was the adaptive filter according to LMS algorithm. Another method has been designed the adaptive filter based on NLMS algorithm. As we described in the preceding sections, the objective of this paper is mitigation of the effect of spoofing signal in GPS receiver. In both methods, we employed the adaptive filter with length of 8 and the step size of μ=0.0003. The next figures show simulation results of the visible satellites in the acquisition, navigation positioning and achieved error. In these figures, we will analyze the results of the two described methods on the measured data set with the spoofing error of 492 meters.

Fig. 3 shows the number of reliable satellites in absent of spoofing signal. This figure is achieved from acquisition stage of a GPS receiver. In the figures, green color displays identified satellites as for the acquisition stage. Hence, as it is displayed in Fig. 3, 5 satellites are reliable in this figure. The simulation is arranged that each green satellite is not applied as effective satellite. Rather only 5 satellites are preferred with upper levels and the receiver be capable to trace 5 satellites. Also, satellites can be tracked that their levels are higher than threshold 5.8. At least, 4 satellites are necessary for the receiver to calculate navigation solution or PVT. As shown in Fig. 3, PRNs 1, 20, 23, 31 and 32 are observable based on the most level in absent of spoofing signal.

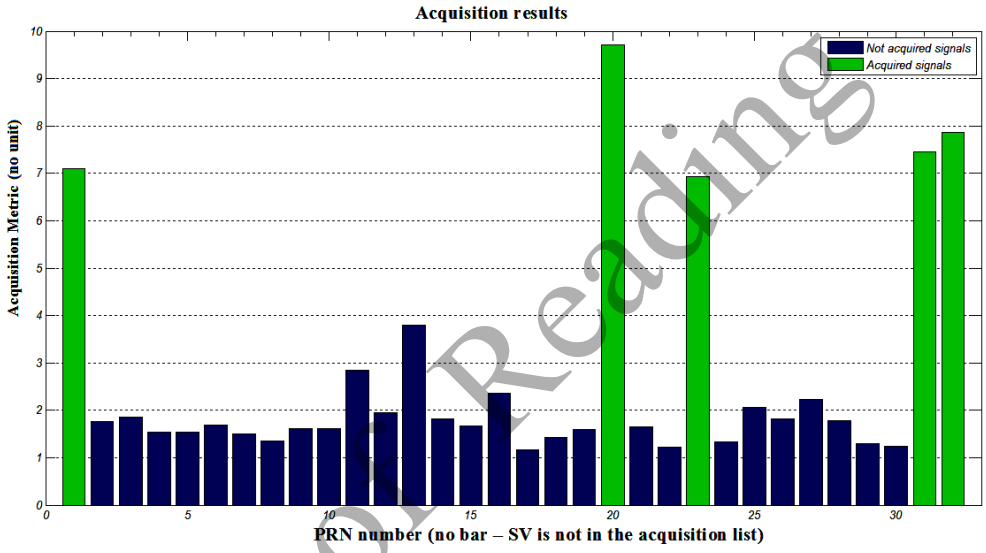

Fig. 3 Reliable satellites with no spoofing.

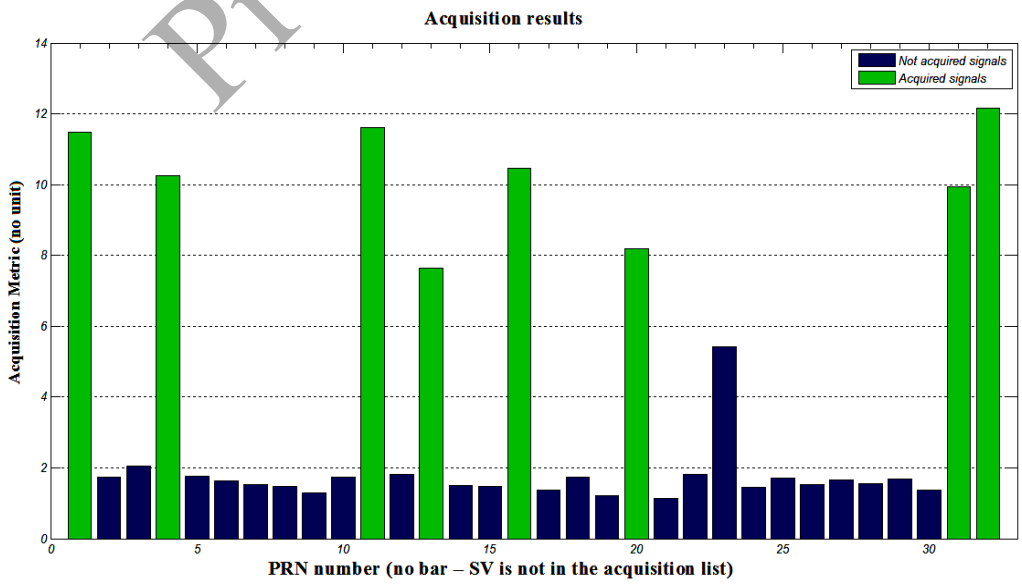

Fig. 4 Detectible satellites during a spoofing attack.

Fig. 4 illustrates 8 acquired satellites throughout the spoofing signal. Thus, PRNs 1, 4, 11, 13, 16, 20, 31 and 32 are observable based on the most level in Fig. 4. According to Fig. 5, PRNs 1, 4, 11, 13, 16, 20, 23, 31 and 32 are visible after applying of the LMS algorithm during spoofing attack. Therefore, the LMS algorithm causes that PRN 23 is visible in acquisition stage. As mentioned above, the 5 satellite of greater levels are preferred as the suitable satellites for processing on the tracking stage of a GPS receiver. Based on Fig. 4, the PRN 20 is not involved the 5 satellites during the interference attack, but after applying LMS algorithm, it is selected as effective satellite owing to its high level. Also, the PRN 11 is consisted of 5 powerful satellites throughout the spoofing attack, however after applying LMS process, it is not considered in Fig. 5. It is obvious from this figures that level of all the satellites has altered after applying spoofing mitigation approach than spoofing attack.

Fig. 6 indicates that PRNs 1, 4, 11, 13, 20, 23, 31 and 32 are detectible after applying performance of the NLMS algorithm based on the utmost level in acquisition stage. In evaluation with state of the spoofing attack in Fig. 4, the PRNs 16 has been removed in Fig. 6. The PRNs 4, 11 and 16 are involved the 5 powerful satellite during the spoofing attack, but in Fig. 6, are not considered. As displayed in Fig. 4 the PRNs 13, 20 and 23 are not contained the 5 satellites, but in Fig. 6, they are considered as effective satellite owing to their high level. In short, PRN 23 is detected in the two approaches of spoofing mitigation. Also, after the LMS algorithm, the PRNs 4 and 16 and after the NLMS algorithm, the PRNs 4, 11 and 16 are chosen as the reliable satellite.

The operation of the GPS navigation solution concludes the three-dimensional (in latitude and longitude and height) geographical location x=(x, y, z) of the GPS receiver from measurements of at least four pseudo-range [30]. The pseudo-range is the distance from the transmitter stations to the receiver. The arrival time of each signal is utilized to compute the pseudo-range. Time of arrival is an amount measure of the intervals to satellite offset by the measure to which the receiver clock is offset from GPS time.

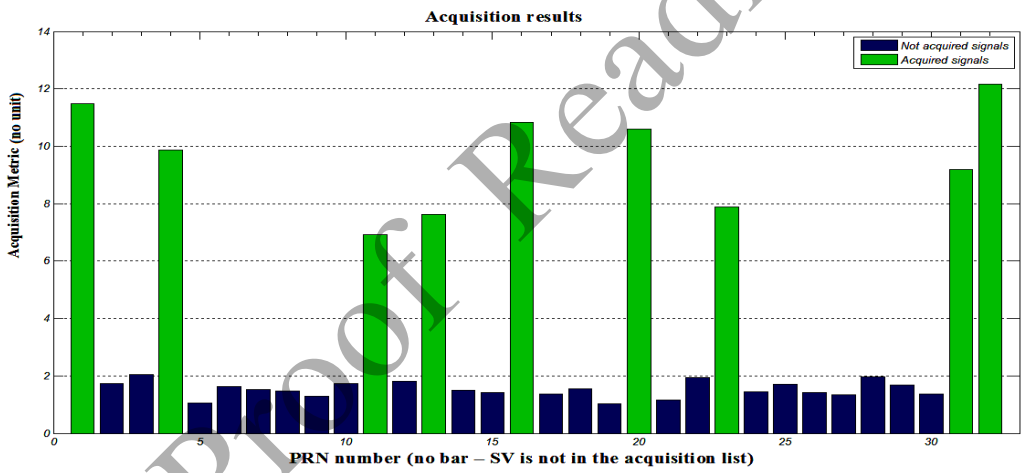

Fig. 5 Observable satellites throughout the spoofing attack after using LMS algorithm.

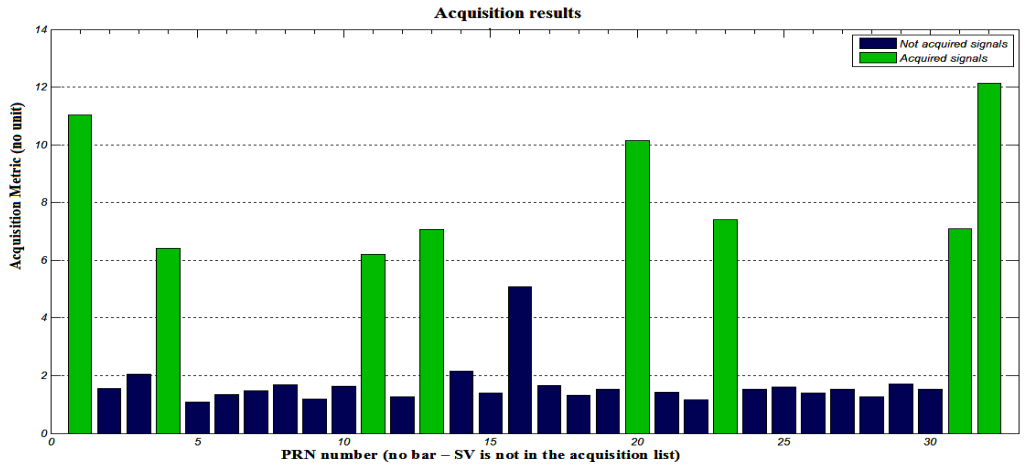

Fig. 6 Observable satellites throughout the spoofing attack after using NLMS algorithm.

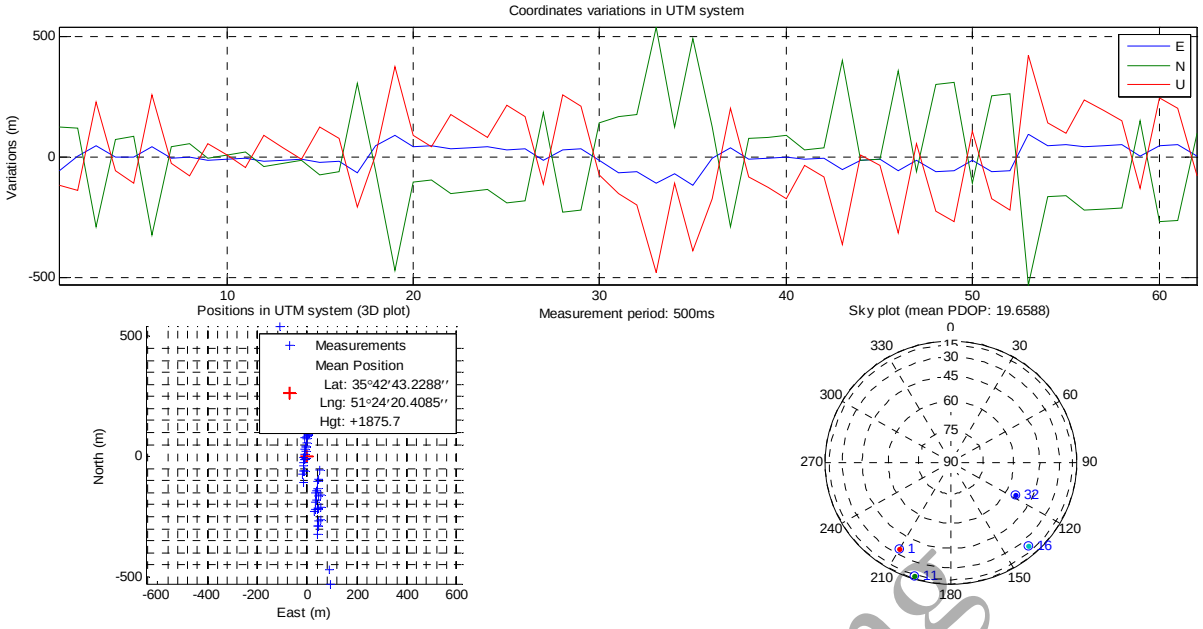

Fig. 7 Location and PDOP during a spoofing attack.

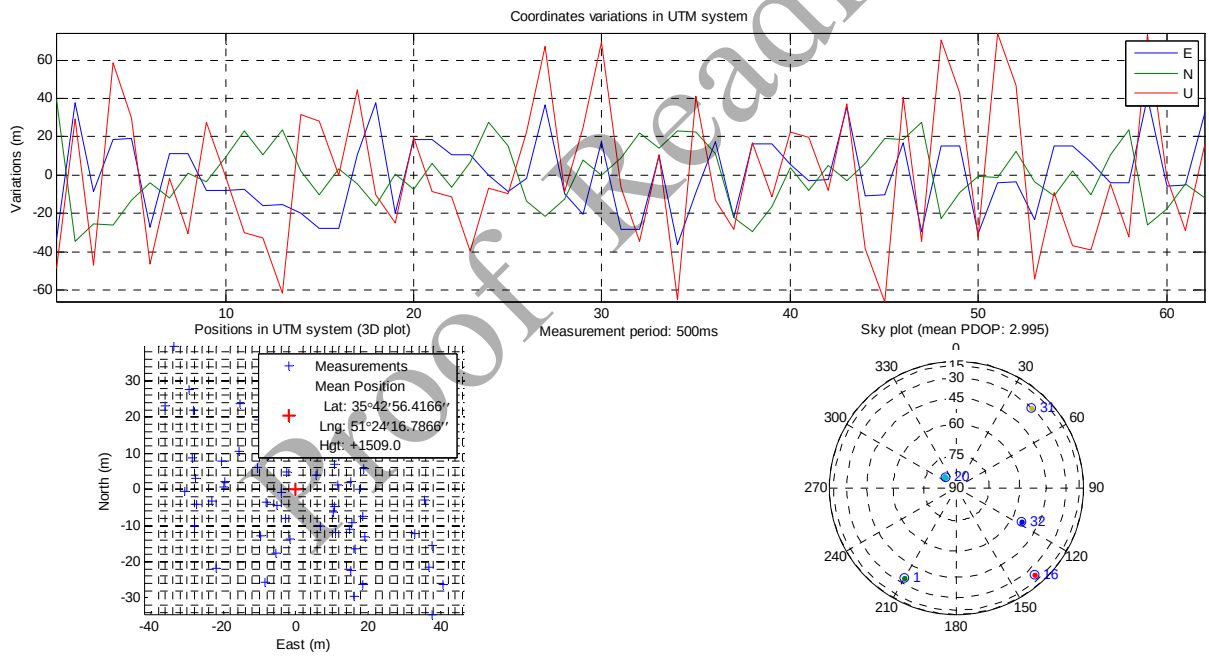

Fig. 8 Location and PDOP during a spoofing attack after using LMS algorithm.

The outcomes of the navigation solution are presented in Figs. 7, 8 and 9. These results were acquired in Universal Transverse Mercator (UTM) system. In this study, the GPS receiver shows situations in UTM coordinates. The UTM system is a pattern of coordinates that simplifies location on a drawing. Fig. 7 illustrates the three-dimensional location in latitude and longitude and height and PDOP measure through a spoofing attack [15]. The GPS receiver display situation of satellites and the PDOP amount in sky plan. PDOP parameter follows mathematically from the places of the operative satellites. Low amount of the PDOP parameter shows the better spatial places of satellites. As is clear from Fig. 7, the PDOP measure is 19.6588 during spoofing attack. As shown in Fig. 8, PDOP amount is decreased to 2.995 after applying LMS algorithm. Briefly, in the new approach using LMS, the term of the Root Mean Square (RMS) error reached from 492 meters to 71 meters. Lastly, we succeeded at least 86 percent spoofing mitigation in the received signal.

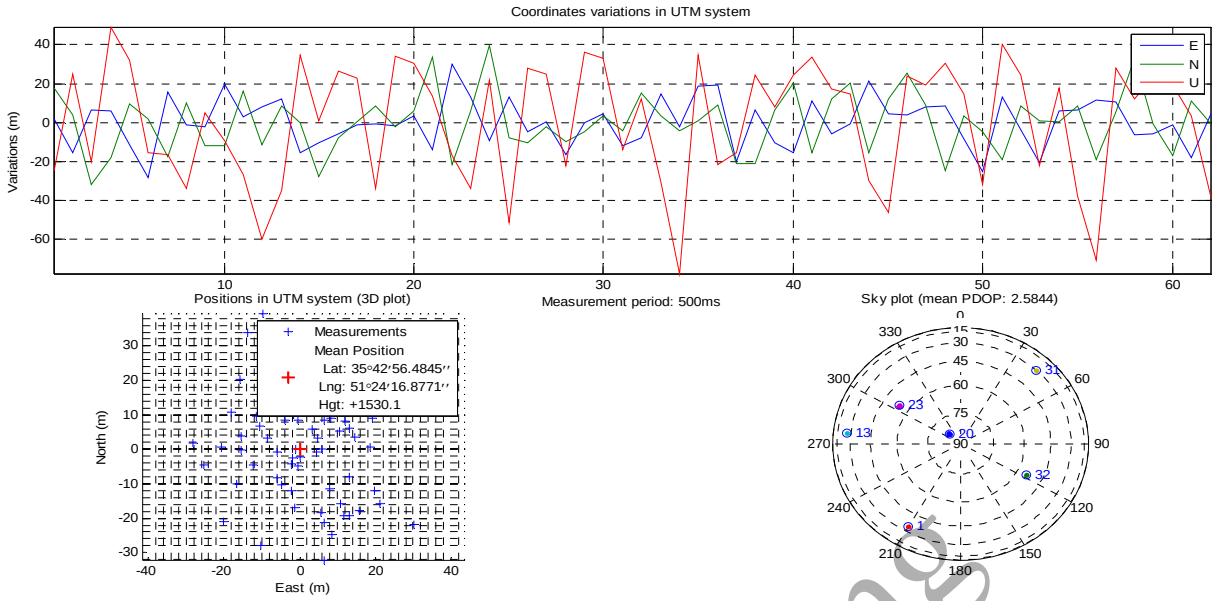

Fig. 9 Location and PDOP during a spoofing attack after using NLMS algorithm.

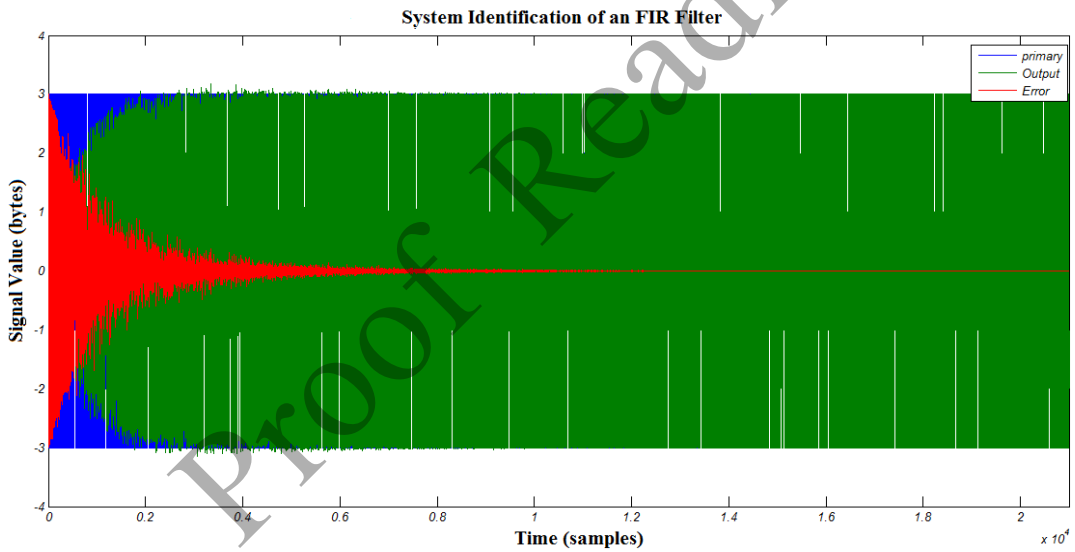

Fig. 10 Primary, output and error signals after using LMS algorithm.

Fig. 9 demonstrates that the usage of NLMS algorithm improves PDOP amount to 2.995. Furthermore, the RMS error is lessened from 492 meters to 53 meters. It is estimated that the implementing this method will offer at least 88 percent spoofing mitigation owing to the received signal.

Figures 10 and 11 show performance of adaptive filter for LMS and NLMS algorithms, respectively. In the both of figures, the primary signal, output signal and the error signal are compared. As it is clear from this figure, the error signal tends towards the value of zero in both methods.

The results for two approaches are summarized in Tables 1 and 2. The presented approaches are performed by a software-defined GPS receiver [30] using a single-frequency approach. The methods were tested on the measured data set for the elimination of spoofing in the GPS received signal. Table 1 expresses the results of LMS algorithm. ΔEN and ΔH parameters show the alterations of the horizontal and height plane, respectively. In this method the best conclusion was achieved on the second dataset that spoofing can be decreased at least 94 percent. At the all results, PDOP amount was significantly improved. The operation of this approach is nearly 84 percent spoofing mitigation on the measurement data set.

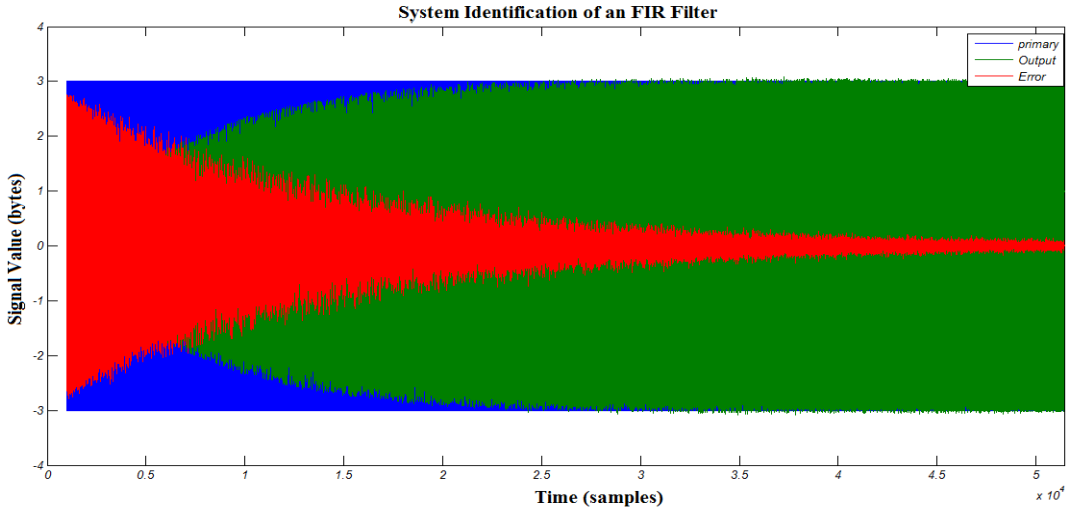

Fig. 11 Primary, output and error signals after using NLMS algorithm.

Table 1 LMS algorithm results on four measured spoofing data sets.

Spoofing data	after algorithm				before algorithm				Spoofing mitigation %
	ΔEN (m)	ΔH (m)	RMS (m)	PDOP	ΔEN (m)	ΔH (m)	RMS (m)	PDOP	
First dataset	50	15	52	3	363	313	479	21	89
Second dataset	22	34	40	3	569	346	666	103	94
Third dataset	28	65	71	3	389	301	492	43	86
Fourth dataset	59	10	60	4	103	155	186	5	68

Table 2 NLMS algorithm results on four measured spoofing data sets.

Spoofing data	after algorithm				before algorithm				Spoofing mitigation %
	ΔEN (m)	ΔH (m)	RMS (m)	PDOP	ΔEN (m)	ΔH (m)	RMS (m)	PDOP	
First dataset	35	64	73	2	363	313	479	21	85
Second dataset	32	20	37	2.5	569	346	666	103	95
Third dataset	29	43	53	2.5	389	301	492	43	88
Fourth dataset	32	35	47	2.7	103	155	186	5	75

Table 3 Numerical comparison of new approaches in this paper with interference mitigation techniques.

Method	Spoofing mitigation on four spoofing data				Spoofing mitigation on average %
	First dataset	Second dataset	Third dataset	Fourth dataset	
NLMS algorithm	85	95	88	75	85.75
LMS algorithm	89	94	86	68	84.25
Wavelet (bior3.7)	60	75	75	40	62.5

Table 2 implies the consequences of the presented NLMS algorithm. As identified the best result is for the second data set that spoofing be reduced at least 95 percent. The PDOP amount is significantly improved at all of results. This model too reduced the spoofing on average 86 percent on the measurement dataset.

According to the obtained results and investigation in Tables 1, 2, applying NLMS algorithm has better effectiveness than LMS algorithm. LMS algorithm reduced the spoofing almost 84 percent on average and NLMS algorithm mitigated the spoofing almost 86 percent on average.

A comparison provides in Table 3 between spoofing mitigation method based on wavelet (bior3.7) in [31] and new approaches in this paper. According to the obtained results in Tables 3, applying LMS-based methods have better effectiveness than wavelet method.

A summarized comparison provides in Table 4 between the previously discussed interference mitigation algorithms [8] in section 2 and proposed techniques in this paper. The powerful aspects of new approaches are their low complexity.

Table 4 Quantitative comparison of interference mitigation techniques.

Interference mitigation method	Interference feature	Complexity	Effectiveness	Receiver required capability
Vestigial signal detection	The authentic signal is still present and can be detected	High	Medium	Multiple receive channels
Multi-antenna	Interference signals coming from the same direction	Medium	High	Multiple receiver antennas
Navigation message authentication	Not authenticated	High	Medium	Authentication
RAIM	Higher residuals for spoofed measurements	Medium	Medium	-
LMS algorithm	Interference signals coming from the spoofer	Low	Medium	Single frequency
NLMS algorithm	Interference signals coming from the spoofer	Low	High	Single frequency

6 Conclusion

This paper presented methods based on adaptive filter in LMS and NLMS algorithms in order to defense against spoofing. Approaches were applied as spoofing mitigation for GPS application. The new approaches were applied in the acquisition stage of the receiver. The proposed methods had been tested on real interference dataset. Simulation results showed that the proposed methods were appropriate solution to mitigate the spoofing at the received signal. Also, they improved PDOP parameter in the GPS receiver. Low amount of the PDOP parameter shows the better spatial places of satellites. Based on the results, the performance of the NLMS algorithms had better performance than LMS algorithms. This model too reduced the spoofing on average 85.76 percent on the measurement dataset. The proposed method guarantees the accuracy of position, notwithstanding the fake satellites. The powerful aspects of new approaches in this paper are their low complexity.

Acknowledgment

The authors would like to thank Iran National Science Foundation Science deputy of presidency for their valuable support during the authors' research work.

References

[1] M. R. Mosavi, S. Azarshahi, I. EmamGholipour and A. A. Abedi, "Least Squares Techniques for GPS Receivers Positioning Filter using Pseudo-range and Carrier Phase Measurements", *Iranian Journal of Electrical and Electronic Engineering*, Vol. 10, No. 1, pp. 18-26, 2014.

[2] M. R. Azarbad and M. R. Mosavi, "A New Method to Mitigate Multipath Error in Single-Frequency GPS Receiver with Wavelet Transform", *Journal of GPS Solutions*, Vol. 18, No. 2, pp. 189-198, 2014.

[3] M. R. Mosavi, "Comparing DGPS Corrections Prediction using Neural Network, Fuzzy Neural Network and Kalman Filter", *Journal of GPS Solutions*, Vol. 10, No. 2, pp. 97-107, May 2006.

[4] F. Shafiee and M. R. Mosavi, "Narrowband Interference Suppression for GPS Navigation using Neural Networks", *Journal of GPS Solutions*, DOI 10.1007/s10291-015-0442-8, 2015.

[5] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen and G. Lachapelle, "GPS Spoofer Countermeasure Effectiveness based on Signal Strength, Noise Power and C/No Observables", *International Journal of Satellite Communications and Networking*, Vol. 30, No. 4, pp. 181-191, May 2012.

[6] M. R. Mosavi and A. A. Akhyani, "PMU Placement Methods in Power Systems based on Evolutionary Algorithms and GPS Receiver", *Iranian Journal of Electrical and Electronic Engineering*, Vol. 9, No. 2, pp. 76-87, 2013.

[7] M. R. Mosavi, M. Pashaian, M. J. Rezaei and K. Mohammadi, "Jamming Mitigation in GPS Receivers using Wavelet Packet Coefficients Thresholding", *IET Signal Processing*, Vol. 9, No. 5, pp. 457-464, 2015.

[8] A. J. Jahromi, A. Broumandan, J. Nielsen and G. Lachapelle, "GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques", *International Journal of Navigation and Observation*, Vol. 2012, Article ID. 127072, pp. 1-16, May 2012.

[9] X. J. Cheng, K. J. Cao, J. N. Xu and B. Li, "Analysis on Forgery Patterns for GPS Civil Spoofing Signals", *4th International Conference on Computer Sciences and Convergence Information Technology*, pp. 353-356, 2009.

[10] S. Daneshmand, A. Jafarnia-Jahromi, A. Broumandan and G. Lachapelle, "A GNSS Structural Interference Mitigation Technique using Antenna Array Processing", *The 8th Sensor Array and Multichannel and Signal Processing Workshop*, pp. 1-6, 2014.

[11] J. Chhikara and J. Singh, "Noise Cancellation using Adaptive Algorithms", *International Journal of Modern Engineering Research*, Vol. 2, No. 3, pp. 792-795, 2012.

[12] A. Elhossini, S. Areibi and R. Dony, "An FPGA Implementation of the LMS Adaptive Filter for Audio Processing", *IEEE Symposium on Field-Programmable Custom Computing Machines*, pp. 324-335, 2006.

[13] K. D. Wesson, D. P. Shepard and T. E. Humphreys, "Straight Talk on Anti-Spoofing Securing the Future of PNT", *GPS World Magazine*, Vol. 23, No. 1, pp. 32-63, 2012.

[14] 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", *ION GNSS Conference*, pp. 1-11, 2011.

[15] M. L. Psiaki, S. P. Powell and B. W. O'Hanlon, "GNSS Spoofing Detection using High-Frequency Antenna Motion and Carrier-Phase Data", *26th International Technical Meeting of the Satellite Division of the Institute of Navigation*, pp. 2949-2991, 2013.

[16] D. P. Shepard and T. E. Humphreys, "Characterization of Receiver Response to Spoofing Attacks", *GPS World Magazine*, Vol. 21, No. 9, pp. 27-33, 2010.

[17] A. Cavaleri, M. Pini, L. Lo Presti and M. Fantino, "Signal Quality Monitoring Applied to Spoofing Detection", *the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation*, pp. 1-9, 2011.

[18] A. Cavaleri, M. Pini, L. Lo Presti and M. Fantino, "Signal Quality Monitoring Applied to Spoofing Detection", *the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation*, pp. 1-9, 2011.

[19] J. Nielsen, V. Dehghanian and G. Lachapelle, "Effectiveness of GNSS Spoofing Countermeasure based on Receiver CNR Measurements", *International Journal of Navigation and Observation*, Vol. 2012, Article ID. 501679, pp. 1-9, 2012.

[20] K. Borre and K. Dragūnas, "Multipath Mitigation based on Deconvolution", *Journal of Global Positioning Systems*, Vol. 10, No. 1, pp. 79-88, 2011.

[21] B. M. Ledvina, W. J. Bencze, B. Galusha and I. Miller, "An In-Line Anti-Spoofing Device for Legacy Civil GPS Receivers", *International Technical Meeting of the Institute of Navigation*, pp. 698-712, Jan. 2010.

[22] J. Nielsen, A. Broumandan and G. Lachapelle, "Spoofing Detection and Mitigation with a Moving Handheld Receiver", *GPS World Magazine*, Vol. 21, No. 9, pp. 27-33, 2010.

[23] L. Scott, "Anti-Spoofing and Authenticated Signal Architectures for Civil Navigation Systems", *16th International Technical Meeting of the Satellite Division of the Institute of Navigation*, pp. 1542-1552, 2003.

[24] K. D. Wesson, M. P. Rothlisberger and T. E. Humphreys, "A Proposed Navigation Message Authentication Implementation for Civil GPS Anti-Spoofing", *ION GNSS Conference*, pp. 3129-3140, 2011.

[25] T. Humphreys, "Detection Strategy for Cryptographic GNSS Anti-Spoofing", *IEEE Transactions on Aerospace and Electronic Systems*, Vol. 49, No. 2, pp. 1073-1090, 2013.

[26] K. Wesson, M. Rothlisberger and T. Humphreys, "Practical Cryptographic Civil GPS Signal Authentication", *Journal of the Institute of Navigation*, Vol. 59, No. 3, pp. 177-193, 2012.

[27] K. S. Gaur and M. Rawat, "Implementation of FIR Filter in Frequency Domain and Time Domain for Wireless Communication System", *International Journal of Computer Science and Technology*, Vol. 2, No. 3, pp. 506-512, 2011.

[28] B. Farhang Boroujeny, *Adaptive Filters Theory and Applications*, John Wiley & Sons, University of Utah, USA, 2013.

[29] L. Ge, Sh. Han and Ch. Rizos, "Multipath Mitigation of Continuous GPS Measurements using an Adaptive Filter", *Journal of GPS Solutions*, Vol. 4, No. 2, pp. 19-30, Aug. 2000.

[30] K. Borre, D. M. Akos, N. Bertelsen, P. Rinder and S. H. Jensen, *A Software-Defined GPS and Galileo Receiver*, Birkhäuser, Basel, 2007.

[31] M. R. Mosavi, A. Bazyar and M. Moazedi, "A New Wavelet based Method for Reduction of Spoofing Effect on Single-Frequency GPS Receivers", *Journal of Soft Computing and Information Technology*, Vol. 3, No. 3, pp. 59-68, 2014, (in Persian).

Mohammad-Reza 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 faculty member of Department of Electrical Engineering of IUST as professor. He is the author of more than 220 scientific publications on journals and international conferences. His research interests include circuits and systems design.

Zahra Shokhmzan received her B.Sc. degree in Electrical Engineering from Jundishapur University, Dezful, Iran in 2010 and the M.Sc. degree in Electrical Engineering from Iran University of Science and Technology (IUST), Tehran, Iran in 2015. Her research interests are signal processing.