Iranian Journal of Electrical and Electronic Engineering

Journal Homepage: ijeee.iust.ac.ir

Interference Mitigation of Replay Attacks in GPS Receiver using of Finite Impulse Response Filter

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

Abstract: The vulnerability of civil GPS receiver to interference may be intentional or unintentional. Among all types of interference, replay attack intended as the most dangerous intentional one. The signal structure of replay attack is almost the same with the satellite signal. The interference effects can be reduce with the design of an appropriate filter in the receiver. This paper presents two methods based on Finite Impulse Response (FIR) filter in frequency and time domain to mitigate the interference effect on GPS signals. Designed FIR filter protects GPS against the replay attack. The suggested filter is applied in the acquisition of the receiver. The proposed method has been implemented on collected dataset. The results show that the proposed algorithms significantly reduce interference. Also, they improve Position Dilution of Precision (PDOP) parameter. Based on the results, the FIR filter technique in time domain has better performance than the frequency domain.

Keywords: FIR Filter, Frequency Domain, GPS, Interference Mitigation, PDOP, Time Domain.

1 Introduction

THE Global Positioning System (GPS) provides location and time information in anywhere on the Earth where there is an unobstructed line of sight to four or more GPS satellite [1]. GPS satellites rotate around the Earth and send signals to the Earth. GPS has three segments. The space segment now consists of 32 satellites, each in its own orbit about 11,000 nautical miles above the Earth. The user segment consists of receivers, which you can hold in your hand or mount in your car. The control segment consists of five ground stations, located around, the world that make sure the satellites are working properly. This system provides critical capabilities to military, civil and commercial users around the world. It is maintained by the United States government and is freely accessible to anyone with a GPS receiver. Advances in technology and new demands on the existing system have now led to efforts to modernize the GPS system and implement the next generation of GPS III satellites [2,3].

GPS signals are very weak broadcasted signal over wireless channels, so they are vulnerable to in band interferences. Thus, even a low-power interference can readily deceive receivers in several kilometers [4]. The vulnerability of civil GPS to interference may be intentional or unintentional. Among the types of interference, spoofing intended as the most dangerous intentional interference [5]. 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 [6]. Spoofing is clandestine; so, it is very tasteful attack than both blocking and jamming. Therefore, appropriate mechanisms be employed for detection and interference mitigation in the receiver [7].

Spoofing attacks are roughly divided into simple, intermediate and sophisticated. The first attack is a simple attack by a GPS signal simulator. One of the spoof simple ways attach a power amplifier and an antenna to the GPS signal simulator and radiates the Radio Frequency (RF) signal toward the target receiver. However, this attack is easy to install, there are some drawbacks for a spoofing attack with a signal simulator. The first is the issue of costs. Modern simulators price is

Iranian Journal of Electrical & Electronic Engineering, 2017.
Paper first received 23 July 2017 and accepted 02 December 2017.
* The authors are with the Department of Electrical Engineering, Iran University of Science and Technology, Narmak, Tehran 13114-16846, Iran.
E-mails: z_shokhmzan@elec.iust.ac.ir, M_Mosavi@iust.ac.ir and moazedi@elec.iust.ac.ir.
Corresponding Author: M. R. Mosavi.

expensive. Another problem is the physical size; most simulators are heavy and bulky. Threat posed by a GPS signal simulator-based spoofing attack is easy to detect. This is because of synchronization a simulator's output with the real GPS signals in its vicinity is difficult. An unsynchronized attack effectively acts like signal jamming, and may lead to the victim receiver to lose lock and have to undergo a partial or complete re-acquisition [8].

The second attack is the intermediate attack via portable receiver-spoofer. The receiver-spoofer can be made small enough to be placed indefinitely on the side of the target receiver's antenna. The receiver-spoofer receives the genuine GPS signal to estimate its own Position, Velocity, and Time (PVT), because it is almost close to the main receiver [9]. According to the estimated PVT, receiver-spoofer produce fake signals and create a spoof attack. If the target were static and its position relative to the receiver-spoofer had been pre-surveyed, the portable receiver-spoofer could even be placed somewhat away from the main receiver [10].

The third attack is sophisticated attack via multiple phase-locked portable receiver-spoofers. In fact, this attack consists all of the challenges of installation a single receiver-spoofer attack, with the additional costs of multiple receiver-spoofers and the additional complexity that the inconsistencies to the incoming signals must be stage coordinated. The only defense against such an attack is cryptographic methods [8].

Replay attack is one of the simplest intermediate spoofing attacks. Defense against replay attack on GPS receivers has been considered as a serious issue to safety of GPS applications [11]. This paper presents two approaches based on FIR filter in both frequency and time domains to reduce the interference effect on GPS signals. The remaining part of this paper is organized as follows. Section 2 introduces a brief discussion on different methods for interference detection and mitigation. Analysis of GPS interference signals are described in section 3. In section 4, techniques for interference mitigation in GPS receiver are presented and the FIR filter in frequency and time domains is designed. Section 5 discusses the experimental results on the measured and simulated dataset. Then, concluding remarks are given in section 6.

2 Related Work

Several methods for interference detection and mitigation that have been described in the papers, is as follows. Shepard [12] demonstrated 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 to interference reciprocity. Signal Quality Monitoring (SQM) is the method for multi-path discovery that identifies interference on the tracking receiver [13]. Ledvina et al (2010) used the delta and ratio SQM tests for interference discovery. SQM is inapplicable when counterfeit and authentic signals are almost aligned [8]. To improve performance of this method, several approaches have been suggested.

Afterwards, Ledvina employed an algorithm of Receiver Autonomous Integrity Monitoring (RAIM) to identify and reduce interference in position and navigation issues [14]. RAIM algorithm is an applicative defense versus measurement error of pseudo-range in the GPS receivers. This approach via statistical hypothesis testing detects pseudo-range measurement error and this error is removed from the navigation solution. The examination of statistical hypothesis applied in RAIM depends on modulus of setting a probability of wrong alarm and calculating a threshold according to the probability of discovery. The accuracy of the infrastructure RAIM and its emphasis on examination of statistical hypothesis extends RAIM-similar methods for the interference discovery and reduction [15,16]. This method is efficient in cases where only one or two spoofed measurements are present among several authentic pseudo-ranges. This is also quite effective for the less sophisticated attacks.

Cryptographic techniques enable the receiver to detect valid signals from interference signals with high probability [17]. In 2003, Logan Scott presented a cryptographic anti-spoofing technique according to Spread Spectrum Security Codes (SSSC) [18]. The latest version of this method considers the L1C signal that will be broadcast on Block III satellites, because the L1C signal is not still completed finalized. SSSCs be interleaved with the civil GPS spreading code into the L1C signal channel [19]. The presentment of the SSSCs has insignificant effect on receivers, inasmuch as L1C acquisition and tracking happens on the pilot channel. In the same reference, Scott is also offered Navigation Message Authentication (NMA) method. If SSSC implementation on L1C is impractical, the method of navigation message authentication 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 [20,21]. These methods are reliable but not accessible on civil GPS receivers.

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. High costs and inefficiency in multipath are drawbacks of this method. Thus, the multi-antenna defense is not widely used by commercial GPS companies [22].

Vestigial Signal Defense (VSD) is a method of interference detecting 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 authentic signal, the original receiver uses the software-defined model. First, the receiver copies the incoming digitized front-end signal into a buffer utilized only for vestigial recognition. Then, the receiver selects one of the GPS signals being tracked and removes this signal from the buffer. This is the similar method applied to remove strong signals in battling the near/far problem in spread spectrum multiple access systems, containing GPS. The VSD is depends on the stiffness of degradation the valid signal after prosperous lift off of the delay-lock loop tracking points. The interaction interplay of the interference and valid signals is similar to the interplay of multi-path and direct-path GPS signals. Performance of this method depends on the weakness of authentic GPS signals during a spoofing attack [23]. Moreover, it is inefficient in synchronous attacks and need prior data.

It seems that the GPS system will not provide low cost security by using these methods. Therefore, the necessity of introducing a more accessible technique with higher accuracy is clearly observable. Previous techniques such as VB and VSD have high implementation costs because of adding extra hardware and needing some changes in the GPS receiver operation.

3 Analysis of GPS Interference Signals

We first introduce GPS valid signal transferred from satellite. It follows that the signal transmitted from satellite *k* can be described as:

$$x_k = \sqrt{2Pc}(C^k(t) \oplus D^k(t))\cos(2\pi f_{L1}t) + N_k \quad (1)$$

where P_C is the power of signal with *C/A*, C_k is the *C/A* code sequence assigned to satellite number *k*, D_k is the navigation data sequence, and f_{L1} is the carrier frequency of L_1. N_k is a sequence of independent, identically distributed zero mean Gaussian noise samples with variance σ_2 that models the effects of thermal noise in the RF front-end [20].

We now define type of GPS interference, replay attack, and analyze how our attacker can deceive the locations of GPS receivers. Spoofer-receiver delay original signal to generate interference signals. Because of the interference signal power to be more than the original signal, it is multiplied by a greater number than one. Then combining of the delayed and original signal reaches the GPS receiver. In fact, the received signal is sum of the original and interference signal in the target receiver. As a result, two similar signals are received just from a receiver, but one of these two signals is delayed. The following equation shows the received signal in the GPS receiver after interference. In this equation, y_k is known as the interference signal.

$$y_k = x_k + \alpha x_{k-d} \quad (2)$$

The coefficient $\alpha > 1$ is the delayed signal's amplitude advantage factor and $d > 0$ is the number of samples of interference delay [21]. The interference signal yk arrives at the target receiver with combining of the delayed signal and the authentic signal. As mentioned above, this attack is replay attack. It achieved with the storage and release of delayed signals. This section describes how to implement the mechanism of delay and composition.

The fake signals were created in a software environment by storing, delaying and combining GPS original signals. To generate fake signals first valid GPS signal was saved in a determined interval. Then, the received signal from the antenna with stored signal was combined and it was published. In fact, stored signal was delayed signal. To avoid easy detection at the receiver by methods such as check of the received signal can normalize power level before propagation of the fake signal. According to the above cases, block diagram of production of interference signal is shown in Fig. 1.

4 Proposed Techniques for Interference Mitigation in GPS Receiver

In signal processing, a digital filter is a system that performs mathematical operations on a discrete-time signal to decrease or increase some aspects of signal. A digital filter is specified with transfer function. Analysis of the transfer function can explain how it will respond to different inputs. Hence, designing a filter contains of developing features appropriate to the problem and therefore, generating a transfer function that meets the features.

The transfer function for a linear, time-invariant system can be represented as a transfer function in the Z-domain; if it is causal, next it has the form:

$$H(z) = \frac{Y(z)}{X(Z)} = \frac{b(1) + b(2)z^{-1} + ... + b(N)z^{-(N-1)}}{1 + \alpha(2)z^{-1} + ... + \alpha(M)z^{-(M-1)}} \quad (3)$$

In Eq. (3), the order of the filter is the more than *N* or *M*. This is the universal model of recursive filters with the inputs (numerator) and outputs (denominator), that normally causes behavior of an Infinite Impulse Response (IIR), but if the denominator to be equal to unity i.e. no feedback, thus, this behaves finite impulse response filter. The impulse response, mostly determined *h*[*n*] or hn, is behavioral specification of how a filter will react to the Kronecker delta function [24].

There are two categories of digital filters: IIR and FIR. As shown in Eq. (4), the impulse response of the linear time-invariant FIR filters is the sequence of filter coefficients:

$$y_n = \sum_{k=0}^{n-1} h_k x_{n-k} \quad (4)$$

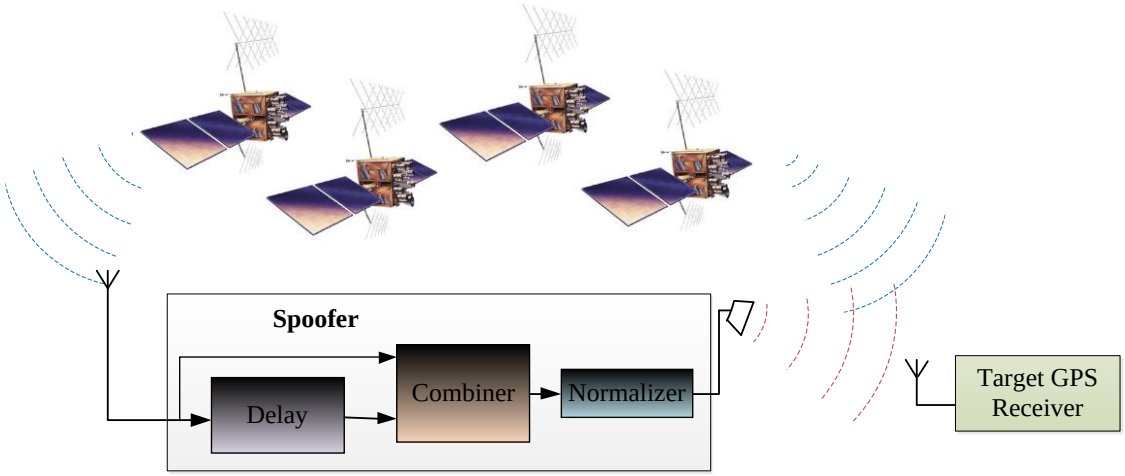

Fig. 1 Block diagram of production of interference signal.

IIR filters are recursive [25]. Output of IIR filters depend on previous outputs and both current and previous inputs. An IIR filter has a general form as Eq. (5):

$$\sum_{m=0}^{M-1} \alpha_m y_{n-m} = \sum_{k=0}^{n-1} b_k x_{n-k} \tag{5}$$

4.1 Design of FIR Filter in Frequency Domain

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 find their position. In this section, the method is presented based on the FIR filters. This method attempts to reduce the effect of the interference in GPS signal. In the section 3, y_k was known as a interference signal in Eq. (2). In this section, yk is used as the signal of filter input. The Fourier transform of Eq. (2) is achieved by Eq. (6):

$$Y_k(e^{jw}) = (1 + \alpha e^{-jwd}) * X(e^{jw}) \tag{6}$$

According to Eq. (6), the transfer function H is defined in Eq. (7):

$$H(e^{jw}) = 1 + \alpha e^{-jwd} \tag{7}$$

In frequency domain the relation between a valid and interference signal is determined by the transfer function $H(e^{jw})$ that input is valid signal and output is interference signal. We need to obtain transfer function that its input and its output be interference signal and valid signal, respectively. According to Eq. (8), we can obtain this transfer function. So, in the Eq. (9), $H1(e^{jw})$ is the desired transfer function. $H1(e^{jw})$ is defined as the inverse of $H(e^{jw})$:

$$X(e^{jw}) = \frac{1}{(1 + \alpha e^{-jwd})} Y_k(e^{jw}) \tag{8}$$

$$H1(e^{jw}) = \frac{1}{1 + \alpha e^{-jwd}} \tag{9}$$

Based on the Taylor expansion can be written $H1$ as Eq. (10). Then, there are two transfer functions for design of digital filter to mitigate interference.

$$H1(ejwd) = 1 - \alpha e^{-jwd} + \alpha^2 e^{-jw2d} + \ldots \tag{10}$$

In section 3, we noted that the coefficient α is the delayed signal's amplitude advantage factor. Therefore α must be a number greater than one since the interference signal power is more than the authentic signal power. Thus in this study α is considered value of 2. At first, the Eq. (10) was used for filter design. It is clear that this transfer function contains an infinite number of exponential functions and it is equivalent to the high-order IIR filter. In fact, to implement this IIR filter, we have approximated it with a FIR filter. For this purpose, we use only a few of the exponential function in this equation. At first, we applied two or three exponential functions of Eq. (10), and so increase this term to achieve the best desired filter. In this report, two, three, four and five terms were examined. The best results are related to using of four and five exponential functions, respectively. The signal of filter output is arrived to different sections of GPS receiver including the acquisition and tracking. Several dataset was investigated and all results reduced the effect of interference in the receiver. Another important result was achieved. After the navigation solution processing, Position Dilution of Precision (PDOP) parameter is significantly reduced and improved. However the proposed filter in Eq. (10) has some problems. It is difficult for the implementation. The run time of processing is long. Whatever the delay be increases, the run time will be longer. To resolve this problem, we use Eq. (9) for the FIR filter design. As before, the effect of interference signal considerably mitigated by such FIR filter at the receiver. Note that the FIR filter is applied to the digital IF signal at the acquisition in the receiver. Fig.2 shows the schematic of used FIR filter in this research. According to the discussed cases, the block diagram of GPS receiver components and location of interference mitigation algorithm are shown in Fig.3.

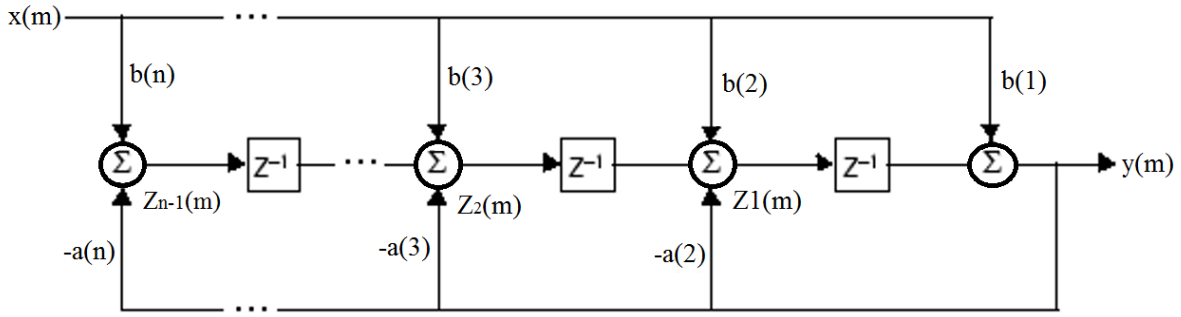

Fig. 2 Illustrating the schematic of used FIR filter in this research.

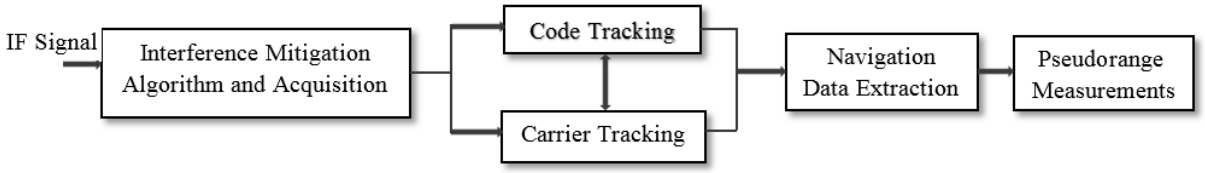

Fig. 3 Block diagram of GPS receiver components and location of interference mitigation algorithm.

4.2 Design of FIR Filter in Time Domain

As previously noted, the Eq. (2) shows the interference signal in the target receiver. In the section 4.1, using the Eq. (2) the FIR filter was designed in the frequency domain. In this section also, we design the appropriate transfer function in the time domain that is presented defense against interference in the GPS signal. The Inverse Fourier Transform (IFT) of $h(e^{iw})$ is $h(n)$. For this purpose, the IFT of Eqs. (9) and (10) are achieved in time domain. Thus, Eqs. (11) and (12) respectively are equivalent transform functions in the time domain.

$$h1_d[n] = \left\{ u[\frac{n}{d}]n \ factor \ d \right\} \tag{11}$$

$$h1[n] = \delta[n] - \alpha\delta[n-d] + \alpha^2\delta[n-2d] - ... \tag{12}$$

Since these two functions are the inverse of transfer function of Eq. (7) in the time domain. As Eq. (13) input and output should be replaced. Therefore, we should note in this study that $y[n]$ as the input and $x[n]$ as output are considered in both time and frequency domains.

$$x[n] = h1[n] * y[n] = \sum_{k=0}^{N} h1[k]y[n-k] \tag{13}$$

In order to reduce the interference, the Eq. (12) has problems. In addition to the mentioned problems in the frequency domain, there is another problem. Implementation of Eq. (12) on all interference data did not lead to interference mitigation. There are an infinite number of impulse functions in this equation and the using of only a few impulse function is not enough in this study. So Eq. (11) is used as the appropriate transfer function. We used the MATLAB software for the simulation. The program is written such that the transfer function is achieved to the first stage. Then, the convolution between interference signal yk and transfer function $h1[n]$ in Eq. (11) is calculated. So, convolution output is considered as an estimate of the valid signal. Finally, the estimated signal arrives to the acquisition in the target receiver.

5 Results

In this section, we discuss the simulation analysis. The results of two proposed techniques are reported and the first method was the design of the FIR filter according to appropriate transfer function in the frequency domain. Another method has been designed the transfer function in the time domain. As we described in the previous sections, the purpose of this study is mitigation of the effect of interference signal in GPS receiver. The following figures have been related to results of the visible satellites in the acquisition and navigation positioning. In these figures, we will analyze the results of the two reported methods on the measured dataset with the interference error of 439 meters. Fig.4 displays the number of authentic satellites without the presence of attack. This figure is obtained from acquisition stage of a GPS receiver. In the figures relating to the acquisition stage green color shows detected satellites. Hence, as it is shown in Fig.4, 5 satellites are authentic in this figure. The simulation is configured that each green satellite is not considered as valid satellite. Rather only 5 satellites are selected with higher levels and the receiver was able to track 5 satellites. Satellites also able to view that their level is higher than threshold 5.8. At least, 4 satellites are required for the receiver to compute navigation solution or PVT. As shown in Fig.4, Pseudo-Random Noises (PRNs) 20, 32, 31, 1 and 23 are respectively visible based on the highest level without the presence of attack.

Fig.5 shows the 9 acquired satellites during the

interference attack. Thus, PRNs 31, 20, 11, 4, 1, 32, 16, 13 and 23 are respectively visible based on the highest level in Fig.5. According to Fig.6, PRNs 20, 11, 1, 32, 4 and 16 are visible after applying of the FIR filter in frequency domain during interference attack. Therefore, the FIR filter performance is caused that PRNs 13, 23 and 31 are not visible in acquisition stage. As mentioned above, the 5 satellites of higher levels are selected as the appropriate satellites for processing at the tracking stage of a GPS receiver. Based on Fig.5 the PRN 32 is not included the 5 satellites during the interference attack, but after FIR filter performance, it is considered as effective satellite due to its high level. Also, the PRN 31 is included 5 effective satellites during the interference attack, but after applying FIR filter in frequency domain, it is not considered. It is clear from this figures that level of all the corresponding satellites has changed during two states.

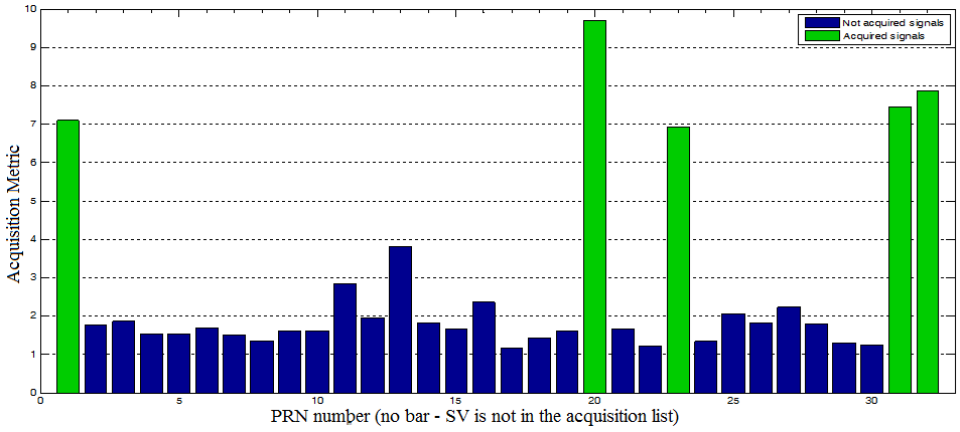

Fig. 4 The authentic satellites without the presence of attack.

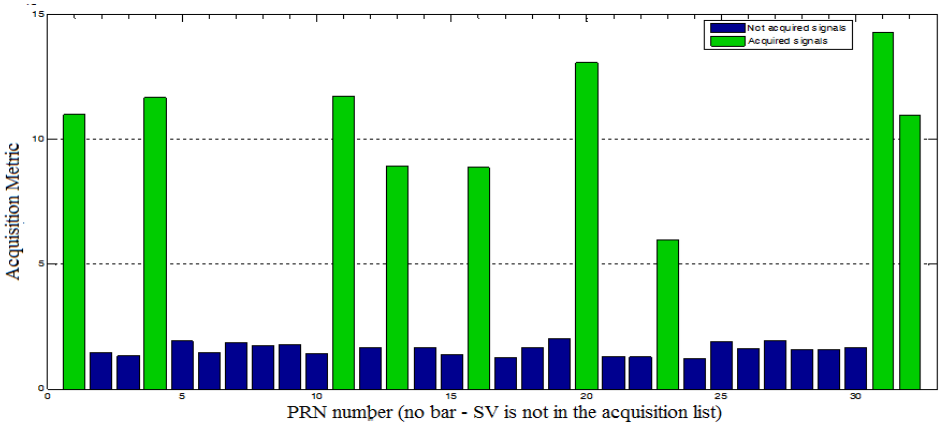

Fig. 5 The visible satellites during an interference attack.

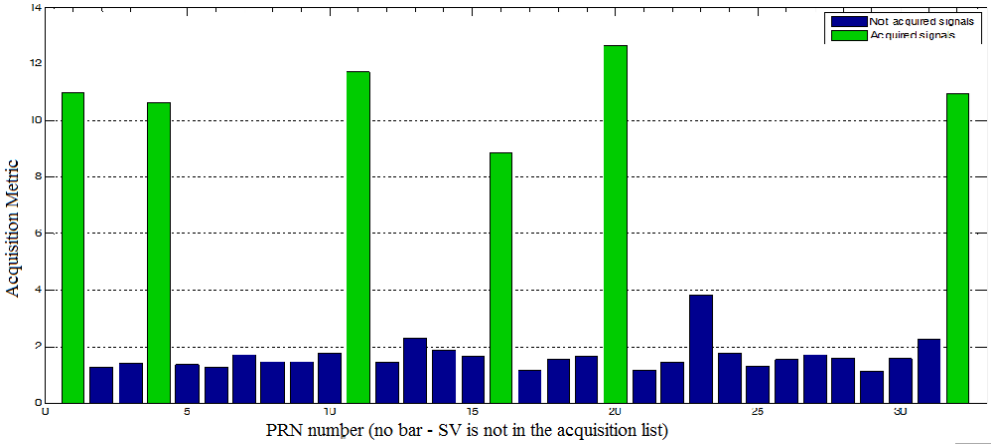

Fig. 6 The visible satellites during an interference attack after applying the FIR filter in frequency domain.

Fig.7 shows that PRNs 31, 4, 32, 20, 1, 11, 13 and 16 are respectively visible based on the highest level in acquisition stage after applying FIR filter in time domain. In comparison with state of the interference attack in Fig.5, the PRNs 23 has been removed in Fig.7. The PRN 11 is included the 5 effective satellites during the interference attack, but in Fig.7, it is not considered. As shown in Fig.5, the PRN 32 is not contained the 5 satellites, but in Fig.7, it is considered as effective satellite due to its high level. Briefly, in the two methods of interference mitigation PRN 23 is removed and the PRN 32 is selected as the authentic satellite.

The GPS navigation solution processing determines the three-dimensional (in latitude and longitude and height) coordinates $x=(x, y, z)$ of the GPS receiver and the clock offset from measurements of at least four pseudo-range [26]. PRN code of the receiver start position at the time of full correlation is the time of arrival of the satellite PRN at receiver. Time of arrival is a measure of the intervals to satellite offset by the amount to which the receiver clock is offset from GPS time. The arrival time of each signal is used to compute the pseudo-range. The pseudo-range is the distance from the transmitter stations to the receiver. The results of the navigation solution are shown in Fig.s 8, 9 and 10. These results were obtained in Universal Transverse Mercator (UTM) system. In this research, the GPS receiver represents locations in UTM coordinates. The UTM system is a system of coordinates that explains position on a map. Fig.8 illustrates the three-dimensional position in latitude and longitude and height and PDOP value during an interference attack [27]. The GPS receiver lets the display of its positions and the PDOP values in sky plot. PDOP be given as a discrete measurements in the three-dimensional position. It follows mathematically from the positions of the operative satellites. Low values of the PDOP parameter indicates a better positional precision, because the wider angular separation between the satellites used to compute a position. As is clear from Fig.8, the PDOP value is 43.8698 during interference attack. As shown in Fig.9, PDOP value is reduced to 8.7244 after using FIR filter in frequency domain that used to mitigation effect of interference. Briefly in method of FIR filter in frequency domain, the improvement in terms of the RMS errors ranged from 439 meters to 40 meters. Finally, we achieved at least 91 percent interference reduction in the received interference signal.

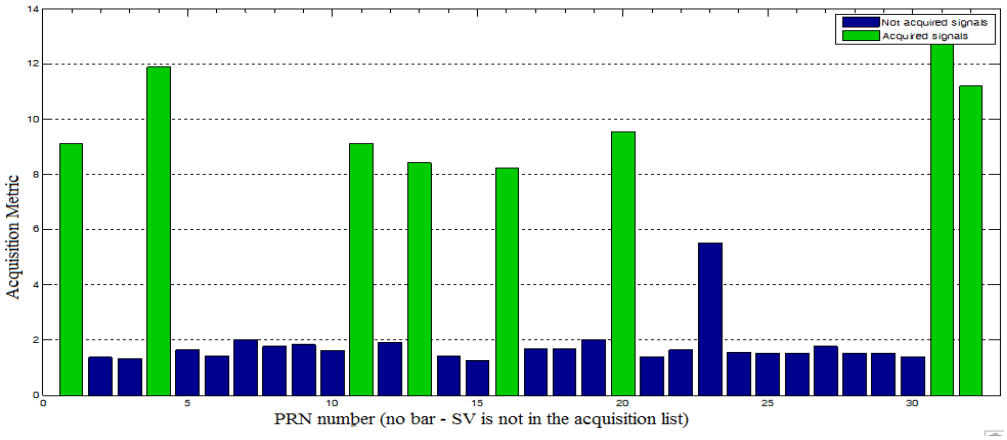

Fig. 7 The visible satellites during an interference attack after applying the time domain FIR filter.

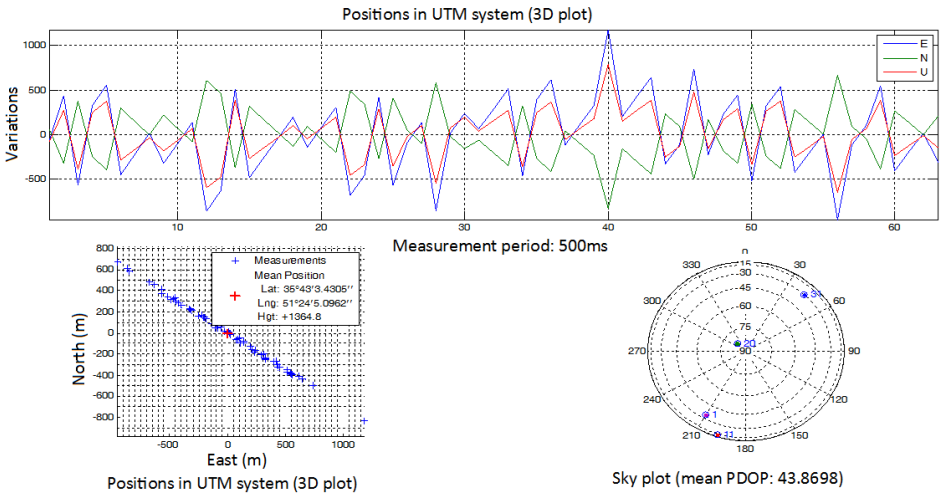

Fig. 8 Illustrating the position and PDOP during an interference attack.

Fig.10 shows that the use of FIR filter model in time domain provided at least a 3 in the PDOP value. Also, the Root Mean Square (RMS) errors are reduced from 439 meters to 62 meters by this model. It is estimated that the use of this model will provide at least 86 percent interference reduction due to the received interference signal.

The following results show details of the two methods that are summarized in below tables. Processing of proposed methods is done by a software-defined GPS receiver [26] in a single-frequency approach. Both the simulated and measured data set were tested in this research. At the proposed methods for the removal of interference in the GPS received signal, we used the transfer function between the interference signal and the valid estimate signal in both frequency and time domain. Tables 1 and 2 show the results on the frequency time domain. ΔEN and ΔH parameters indicate the change of the horizontal and height plane, respectively [26]. In this model, the best result was obtained in Table 2 on the third dataset that interference can be reduced at least 91 percent. At the most results, PDOP value was significantly improved. The performance of this method is almost 60 percent interference reduction on the simulated dataset and 81 percent interference mitigation on the measurement dataset. Our results demonstrate that the proposed method reduces the interference more on the measurement data set than the simulated data set.

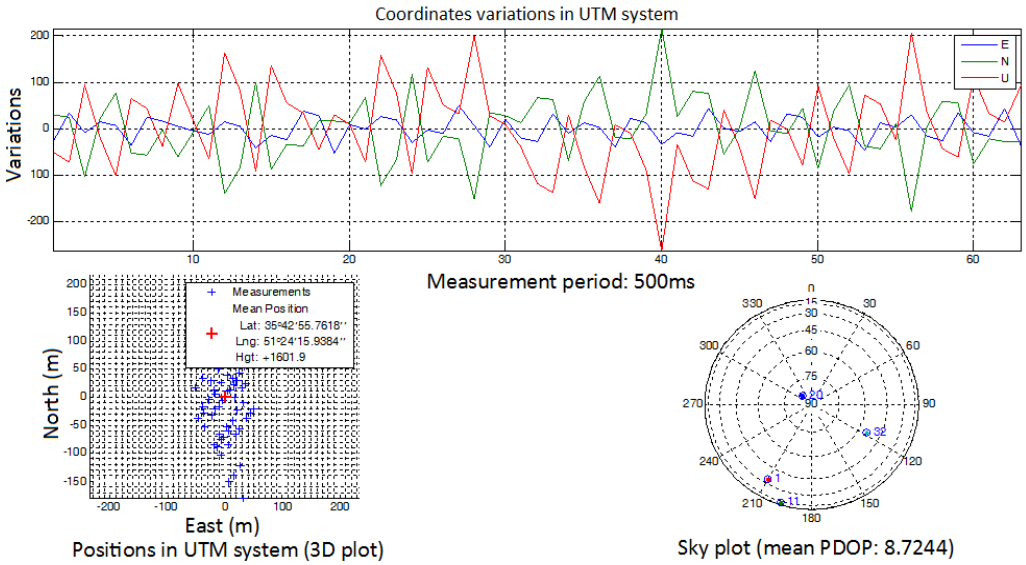

Fig. 9 The visible satellites during an interference attack after applying the FIR filter in frequency domain.

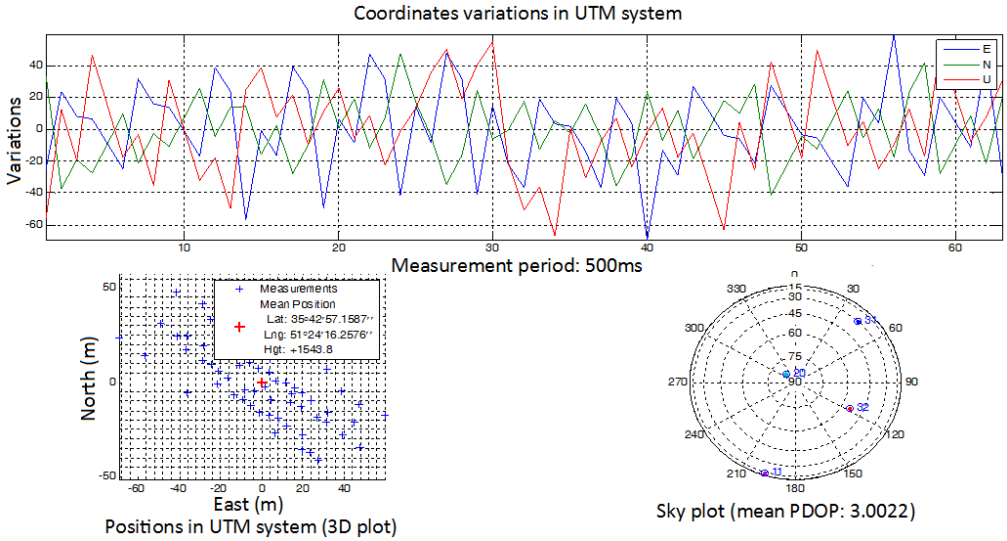

Fig. 10 Illustrating the position and PDOP during an interference attack after applying the time-domain FIR filter.

Tables 3 and 4 show the results of the proposed transfer function in the time domain. As specified the best results are for the first data set and second data set in the Table 4 that interference be reduced at least 87 percent. The PDOP value is significantly decreased at all of results. This model also reduced the interference on average 60 percent on the simulated data set and 83 percent in the measured data set.

According to the obtained results and analysis, design of FIR filter in time domain has better effectiveness and runtime than the frequency domain. Therefore, the time domain approach was selected as batter proposed method.

A summarized comparison provides in Table 5 between the previously discussed interference mitigation algorithms [8] in section 2 and proposed techniques in this paper on the examined factors, required equipment, limitations and advantage of approaches. In order to have a better judgement, a numerical value was assigned to each feature. The worst and the best cases are considered for any feature; score 0 is dedicated for the worst state and 10 score is devoted for the best state. After that, a number ranged 0 to 10 is assigned to any feature depending on the algorithm performance. For example, about the feature "necessary equipment", an algorithm takes 10 if no extra equipment is needed. Besides, in case of necessity to basal changes in receiver structure, it earns 0. As can be seen, the proposed algorithm performs better than others because the offered method needs no extra hardware and does not increase the receiver size and the production costs.

Table 1 The results with and without frequency domain FIR filter for four simulated interference data sets.

Interference data	After algorithm				Before algorithm				Interference reduction %
	ΔEN (m)	ΔH (m)	RMS (m)	PDOP	ΔEN (m)	ΔH (m)	RMS (m)	PDOP	
First dataset	29	20	35	3	9	67	67	8	48
Second dataset	9	12	15	3	16	44	47	7	67
Third dataset	17	3	18	3	41	59	72	7	75
Fourth dataset	9	12	15	3	7	30	31	7	50

Table 2 The results with and without frequency domain FIR filter for four simulated interference data sets.

Interference data	After algorithm				Before algorithm				Interference reduction %
	ΔEN (m)	ΔH (m)	RMS (m)	PDOP	ΔEN (m)	ΔH (m)	RMS (m)	PDOP	
First dataset	29	91	96	3	343	297	454	21	79
Second dataset	57	50	76	2	370	415	556	51	86
Third dataset	29	28	40	8	387	209	439	43	91
Fourth dataset	21	3	21	4	18	62	65	6	68

Table 3 The results with and without time domain FIR filter for four simulated interference data sets.

Interference data	After algorithm				Before algorithm				Interference reduction %
	ΔEN (m)	ΔH (m)	RMS (m)	PDOP	ΔEN (m)	ΔH (m)	RMS (m)	PDOP	
First dataset	29	20	35	2.7	9	67	67	8	48
Second dataset	9	12	15	3.1	16	44	47	7	67
Third dataset	17	3	18	2.8	41	59	72	7	75
Fourth dataset	9	12	15	3	7	30	31	7	50

Table 4 The results with and without time domain FIR filter for four measured interference data sets.

Interference data	After algorithm				Before algorithm				Interference reduction %
	ΔEN (m)	ΔH (m)	RMS (m)	PDOP	ΔEN (m)	ΔH (m)	RMS (m)	PDOP	
First dataset	59	17	61	3	343	297	454	21	87
Second dataset	40	58	70	3	370	415	556	51	87
Third dataset	54	30	62	3	387	209	439	43	86
Fourth dataset	40	22	45	3	29	160	163	9	72

Table 5 Comparison of interference mitigation techniques.

Detection methods	Analyzed features	Required equipment	Advantages	Limitations	Total mark
SQM	Correlation branch (4)	Software upgrade (6)	Easy detection (5)	Inefficient in synchronous attacks and multipath, need prior data (2)	17
VSD	Correlation branch (4)	Software and hardware upgrade (3)	Ability to multipath separation (7)	Inefficient in synchronous attacks, need prior data (5)	19
NMA	Navigation message (3)	Software upgrade and extra hardware (2)	High recognition accuracy (8)	High cost and complexity (3)	16
RAIM	Pseudo-range (3)	Software upgrade (6)	Easy to implement (5)	Unreliable in more than 2 counterfeit satellites (2)	16
Spacial	IF signal (5)	Software upgrade and extra hardware (0)	High reliability (7)	Unreliable in sophisticated attacks (6)	18
This work	Acquisition (5)	Software upgrade (6)	Easy to implement, real-time and reliable (9)	Algorithm needs prior data (5)	25

6 Conclusions

This paper presented methods based on FIR filter in both the frequency and time domain in order to defense against replay attack. FIR filter method was applied as an interference mitigation for GPS application. Replay attack effects was reduced with the design of an appropriate filter in the receiver. Also, the suggested filter was applied in the acquisition stage of the receiver. The proposed methods had been tested on measurement and simulated interference dataset. Simulation results showed that the proposed methods were appropriate solution to mitigate the interference at the received signal. Also, they improved PDOP parameter in the GPS receiver. Based on the results, the performance of the FIR filter technique in time domain had better performance than the frequency domain. The proposed method guarantees the accuracy of position, notwithstanding the fake satellites.

References

[1] M. R. Mosavi, H. Nabavi and A. Nakhaei, "Neural Technologies for Precise Timing in Electric Power Systems with a Single-Frequency GPS Receiver," *Journal of Wireless Personal Communications*, Vol. 75, No. 2, pp. 925-941, 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*, pp. 1-17, 2014.

[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] O. Pozzobon, "Keeping the Spoofs Out: Signal Authentication Services for Future GNSS," *Inside GNSS Magazine*, Vol. 6, No. 3, pp. 48-55, 2011.

[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*, pp. 1-14, 2014.

[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*, 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] 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.

[12] 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.

[13] 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.

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

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

[16] 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.

[17] 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.

[18] 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.

[19] 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.

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

[21] 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.

[22] M. L. Psiaki, M.L. Powell, S.P. O'Hanlon and B.W, "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.

[23] 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.

[24] 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.

[25] Y. Singh, S. Tripathi and M. Pandey, "Analysis of Digital IIR Filter with LabVIEW," *International Journal of Computer Applications*, Vol. 10, No. 6, pp. 23-30, 2010.

[26] K. Borre, D. M. Akos, N. Bertelsen, P. Rinder, S. H. Jensen, *A Software-Defined GPS and Galileo Receiver-A Single-Frequency Approach*, Birkhäuser, Bosten, 2007.

[27] N. Rahemi, M. R. Mosavi, A. A. Abedi and S. Mirzakuchaki, "Accurate Solution of Navigation Equations in GPS Receivers for Very High Velocites using Pseudo-range Measurements," *Journal of Advances in Aerospace Engineering*, Vol. 2014, pp. 1-8, 2014.

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

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 faculty member (professor) of the Department of Electrical Engineering of IUST. He is the author of more than 330 scientific publications in journals and international conferences. His research interests include circuits and systems design.

M. Moazedi received her B.S. and M.S. degrees in Electronic Engineering from IUST, Tehran, Iran in 2008 and 2011, respectively. She is currently Ph.D. student of IUST Department of Electrical Engineering. Her research interests in the area of analog and mixed signal integrated circuits, GPS security and integrity.