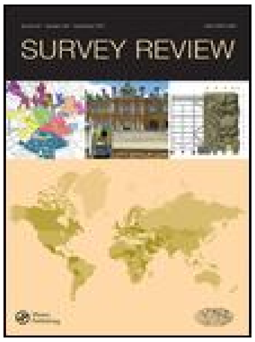


Survey Review

ISSN: 0039-6265 (Print) 1752-2706 (Online) Journal homepage: http://www.tandfonline.com/loi/ysre20

Robust acquisition at GPS receivers in unsafe locations using complex wavelet transform

M. Moazedi, M. R. Mosavi & A. Sadr

Robust acquisition at GPS receivers in unsafe locations using complex wavelet transform

M. Moazedi, M. R. Mosavi[*] and A. Sadr

Growing importance of Global Positioning System (GPS) applications in various fields, leads many researches to the security of GPS systems and investigation of eventual perturbations in them. One of the most important intentional interferences is spoofing. This work presents an anti-spoofing method based on complex wavelet transform (CWT). Fake satellites are omitted and then understrength satellites due to spoofing are identified. The results of investigation suggest that the proposed CWT based estimation and extraction method is better than relatively simple wavelet transform. The suggested filter is applied in the Intermediate Frequency signal. Cross-validation technique is used for automatically identifying wavelet signal layers. The proposed method has been implemented on different collected datasets. Software GPS Receiver has been used to implement and validate the developed anti-spoofing technique because it is more flexible and economical compared with usual hardware receivers.

Keywords: Complex wavelet transform, GPS receivers, Interferences, Robust acquisition, Dual-tree, Acquisition

Introduction

The free availability of the Global Positioning System (GPS) since 1980 and its accuracy for positioning and timing, combined with the low cost of receiver chipsets, has caused a growing number of GPS applications for localisation, navigation, time synchronisation, mapping and tracking. Moreover, civilian GPS signals are unencrypted, predictable and low power ones. These made them vulnerable to RF interference (Warner and Johnston 2002). As shown in Fig. 1, spoofing is the transmission of fake GPS signals that receivers accept as authentic ones (Bonebrake and O'Neil 2014). By showing the vulnerability of civil GPS receivers to interference, the researchers try to devise methods for protecting against attacks like spoofing. One of the effective approaches to counterfeit spoofing is to track the encrypted Y-code. Unfortunately, this is possible by using a GPS receiver including Selective Availability Anti-Spoofing Module (SAASM) (Kaplan and Hegarty 2007). In the SAASM receivers, proper mechanisms are employed for spoofing detection and mitigation in the GPS receiver.

GPS receiver can be vulnerable to spoof signals in distinct operative levels such as antenna and front-end level, acquisition, tracking loop and positioning solution or pseudo-range. With taking into this consideration, countering acts can be done in different GPS operative levels (Jahromi *et al.* 2012a).

Acquisition is the first signal processing operation performed on the Intermediate Frequency (IF) GPS signal (Mosavi and Shafiee 2016). Acquisition identifies the Line-of-Sight (LOS) satellites and estimates the Doppler frequency and delay in Coarse/Acquisition (C/A) code of the satellite signals. In the next step, tracking is performed through parallel channels based on acquisition measurements. Therefore, the performance of acquisition processes directly influences the performance of tracking operation (Ahmad *et al.* 2016).

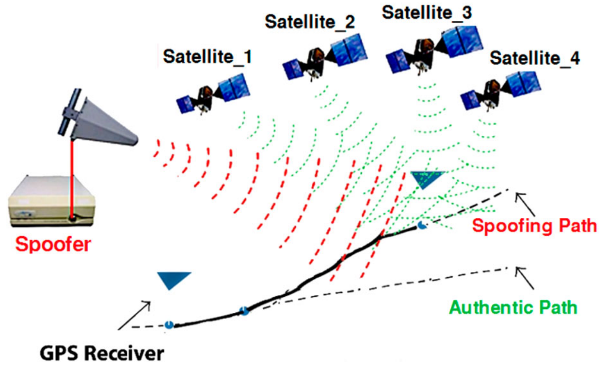
So far, various methods have been proposed to deal with spoofing. From the most important interference detection techniques can be noted to Signal Quality Monitoring (SQM) (Mitelman 2004), Vestigial Signal Defense (VSD) (Wesson *et al.* 2011), Vector Base (VB) GPS receiver (Jahromi *et al.* 2012b) and detection based on carrier to noise ratio (Motella *et al.* 2010). In the case of spoof reduction, it can be mentioned to using VB receiver, authentic signal estimation by the predictor such as Kalman filter (Jwo and Lai 2008) and Receiver Autonomous Integrity Monitoring (RAIM) (Ledvina *et al.* 2010). Some countermeasures are mainly based on constantly investigating and comparing the internal and external information, and then estimating of authentic signal (Kwon *et al.* 2014). Adaptive filter is used for estimating the parameters of authentic and forgery signals (Mosavi *et al.* 2016).

A desirable criterion for anti-spoofing algorithms is that it can be added to civil GPS receivers easily. In contrast to previous methods, the necessity of introducing a new spoof mitigation algorithm that can be implemented simply in civil GPS receiver is clearly observable. Here, we have introduced a novel technique for GPS data processing based on wavelet transform (WT). Techniques based on WT, have been extensively used in data compression, signal processing, data analyses in engineering, finance, science, etc.

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

[*]Corresponding author, email m_mosavi@iust.ac.ir

Received 11 February 2018; accepted 29 May 2018
DOI 10.1080/00396265.2018.1483597



1 Deviation of GPS receiver from the original path

First, Ref. (Collin and Warnant 1995) used WT in order to slip correction of GPS cycle. Fu and Rizos 1997 reviewed several applications of wavelets to GPS data processing (Fu and Rizos 1997). Ogaja *et al.* introduced the WT to analyse the GPS results in a structural monitoring application (2001). Satirapod *et al.* applied different wavelets to separate the systematic error component from the noise component in the GPS double differenced residuals (2003). The Ref. (Chien *et al.* 2017) proposes a novel anti-jamming architecture, combining wavelet packet signal analysis with adaptive filtering theory to mitigate chirp interference. WT has also been used in repeat-time based interference mitigation for GPS receivers (Lawrence 2017). A wavelet packet transform-based adaptive predictor with a new adaptive threshold selection algorithm is proposed newly (Chien 2018). A novel GPS signal acquisition scheme based on discrete wavelet transform (DWT) is proposed to improve acquisition performance (Ahmad *et al.* 2016).

The next section dedicated to study of complex wavelet transform (CWT). Then we will propose the spoofing detection and reduction approach based on CWT. Four rooftop-collected data sets used in performance assessment of the proposed method, are described later. After that, processing results and their interpretation are discussed. Some general conclusions are drawn at the end of the paper.

Complex wavelet transform

CWT will be shortly introduced here. WT is a helpful tool for processing of non-stationary and transient signals such as GPS signals, (Mosavi and Emamgholipour 2013). A significant aspect of WT is high precision in both of time and frequency resolution. Indeed, it presents an alternative to standard Fourier Transform (Azarbad and Mosavi 2014).

Wavelet packets provide a general representation of multi-resolution decomposition and include the entire family of sub-band coded (tree) decompositions. The inverse of this transform has the perfect reconstruction (PR) property. The WT suffers from four fundamental, interweaved shortcomings: (1) oscillations, (2) shift variance, (3) aliasing and (4) lack of directionality (Kingsbury 2001). Fortunately, a simple solution exists for all of these shortcomings. The main aspect is that Fourier Transform is not faced with these problems. It is based on complex-valued oscillating sinusoids as

$$e^{i\Omega t} = \cos(\Omega t) + j\sin(\Omega t) \qquad (1)$$

Based on FT, a CWT is represented as

$$\psi_c(t) = \psi_r(t) + j\psi_i(t) \qquad (2)$$

where $\psi_\mathrm{r}(t)$ is real and even and $j\psi_i(t)$ is imaginary and odd. The complex scaling function can be defined similarly. Projecting the signal onto $2^{j/2}\psi_\mathrm{c}(2^j t{-}n)$ the complex wavelet coefficient is resulted as

$$y_c(j,n) = y_r(j,n) + jy_i(j,n) \qquad (3)$$

$$|y_c(j,n)| = \sqrt{|y_r(j,n)|^2 + |y_i(j,n)|^2}$$
$$\angle y_c(j,n) = \arctan\left(\frac{y_i(j,n)}{y_r(j,n)}\right) \qquad (4)$$

The energy in the wavelet domain is equal to the energy of the input signal:

$$\sum_{j,n}(|y_h(j,n)|^2 + |y_g(j,n)|^2) = \sum_n |x(n)|^2 \qquad (5)$$

As with Fourier Transform, CWT can be used to analyse and represent both real and complex-valued signals. Both $\psi_r(t)$ and $\psi_i(t)$ form orthonormal or biorthogonal bases. We will focus on a dual-tree approach, the redundant type of CWT. It is based on two Filter Bank (FB) trees and thus two bases.

Robust acquisition

One of the most significant responsibilities of a GPS receiver is the determination of LOS satellites such that positioning error be minimised. The selection process plays a critical role in the whole positioning process. Therefore, if satellites are selected inappropriately, the final positioning will not be reliable. Spoofing can affect the acquisition process in two different ways. First, the spoofer generates one or more fake correlation peaks and these peaks take the place of the real ones. Second, the spoofer can manipulate the acceptable satellites by the receiver. It will be shown that monitoring the features of received GPS signals during the acquisition process is highly effective to reduce receiver vulnerability to spoofing attack.

Fake satellites identification

Generally, feature detection is used to isolate or extract important information of a signal. Wavelets are well in detecting and isolating certain features appearing in the signal. This is essential for the suggested CWT based algorithm in retrieving the spoof signal from received data. The experiences are verified on acquisition process of a software GPS receiver, on which external disturbances are presented in the form of high wavelet coefficients.

The detection process must own good indicator properties for successful detection: all real features should be isolated, and false warnings should be minimum. There is another requirement for successful on-line detection: fast detection. Building dedicated waveforms can improve the results, and the real-time algorithm provides fast spoof detection, which is helpful to minimise execution loss. On the other hand, if the feature can be detected totally, detection accuracy will be optimal. Therefore, a trade-off between accuracy and speed should be considered. Proposed on-line wavelet-based feature detection technique used the real-time wavelet analyser.

The latter step is designing a decision rule based on information of the indicator that can decide whether a feature is detected or not. In the case of our approach, the decision rule is a threshold. A fake satellite has a large first peak in the acquisition process. The feature will be identified if the coefficient value of a certain level rises above the specified threshold. After omission of counterfeit satellites, we will try to identify the conk out satellites due to spoofing in the next section.

Satellite existence verification

A Satellite Existence Verification (SEV) process for detecting low power GPS signals due to spoofing attack is presented in the acquisition process. This is based on the time–frequency presentation of GPS signal while the signal is absent. The SEV method assists the acquisition process of GPS signal in detection of low power signal, without making a change in the original signal acquisition algorithm. In this way, acquired GPS satellites could be increased to continue the navigation process.

The GPS L1 signal received from the kth satellite in the front-end can be described as (Kaplan and Hegarty 2007):

$$S_{L1}^{(k)}[n] = \sqrt{P_c}C^{(k)}[n]D^{(k)}[n]\cos[\omega_{IF}n] + e[n] \tag{6}$$

where Pc is signal power, $C[n]$ is the C/A code sequence. D $[n]$ is the navigation message. ω_{IF} is the IF frequency, and n denotes the nth sample of the signal in discrete time representation. $e[n]$ is generally the unwanted signal, which includes interference or noise.

A single trial decision is shown in Fig. 2. The left and right curves in both graphs represent the probability density functions of noise with signal present and absent, respectively. A satellite signal is declared present if the estimated Signal to Noise Ratio (SNR) in the acquisition step is over the threshold. Nevertheless, the black area presents a false alarm of signal. The signal detection process would have a probability of miss-detection (P_{md}). Under the hypothesis 0 of signal absence or code delay/Doppler frequency shift mismatch, the false alarm probability (P_{fa}) is defined (Kaplan and Hegarty 2007) as

$$P_{fa,Vt} = P_{fa}(S(\tau, f_D) > V_t|H_0) \tag{7}$$

$P_{fa,Vt}$ presents the possibility that the decision variable $S(\tau, f_D)$ proceeds a predefined threshold V_t under hypothesis H_0. Inversely, under the hypothesis H_1 the detection probability (P_{det}) is defined as

$$P_{det,V_t} = P_{det}(S(\tau, f_D) > V_t|H_1) \tag{8}$$

$P_{\det,V_t}$ indicates perfect delay, signal presence and frequency alignment between the local replica and the received signal. Normally, a false alarm probability (P_{fa}) is chosen first, and detection probability (P_d) and the corresponding threshold can be estimated. The miss-detection probability (P_{md}) increases until P_{fa} is strict as a typical power signal. Therefore, the satellite with low power signal would be pushed aside while the SNR is below the specified threshold. Therefore, the acquired satellites will be reduced and then might not be sufficient for navigation. In the acquisition process, by multiplying a local replica C/A code generated according to the acquired code delay information, the C/A code is eliminated from the received GPS signal. If the signal existed, the remaining signal with a length of 1 ms would include undesired noise terms and a carrier as

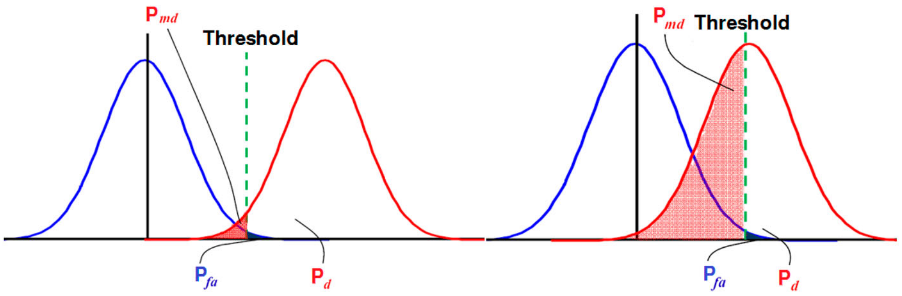
$$S_{L1}^{(k)}[n] = \cos[\omega_{IF}n] + e[n] \tag{9}$$

The navigation information is the same within 1 ms. Afterwards, the remaining signal is mapped into CWT. 1 ms GPS signal sampled at 5.7 MHz is used to perform the algorithms. CWT is utilised to perform the Fast Fourier Transform (FFT) on 2850 points instead of 5700 point FFT without affecting the operation of the acquisition process. Concentrating the signal energy in some coefficients of WT, helps to apply FFT on decreased number of points. This simplifies complexity of the acquisition process. Fig. 3 shows a detailed block diagram of the SEV process for a specific Pseudo Random Noise (PRN). Additionally, the SEV method would be performed the following acquisition stage when the SNR of a satellite signal is under and near to the threshold Vt.

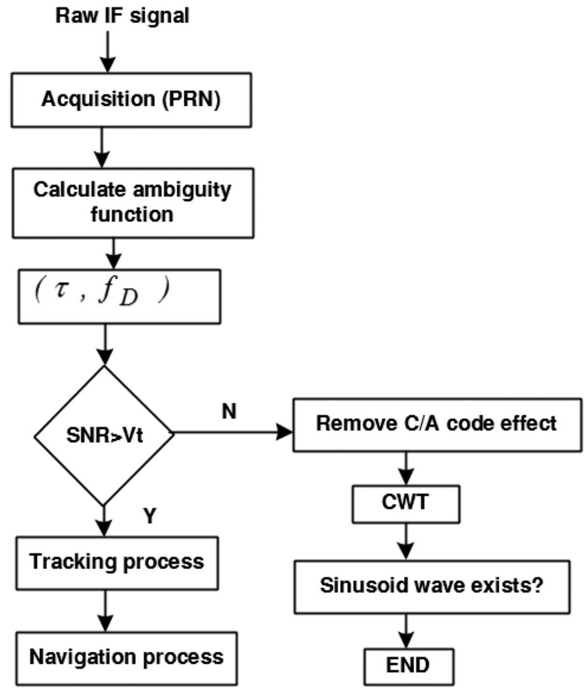
After the wavelet decomposition, a cross-validation technique is used to identify automatically signal levels of the wavelet-decomposed (Arlot and Celisse 2010). The basic concept of cross-validation is to cross-validate filtered results with data samples (Zhong *et al.* 2008). The proposed algorithm is implemented as:

Step 1: Dividing the observational data series (x_i, y_i), i = 1, 2, … N into two parts, the even series ($x_{2,2m}$, $y_{2,2m}$) m = 1, 2, … N_1 and odd *series* ($x_{1,2m-1}$, $y_{1,2m-1}$). The even series is sampled randomly as the validation series, and odd series is referred to as the filtering series.

Step 2: Utilising wavelet decomposition of K-level in the filtering series. In this way, the filtered values at the kth level are obtained. Now, the variance of the validation



2 **Typical strength GPS signal detection in acquisition process (left) and received power GPS signal detection in acquisition process (right)**



3 **Block diagram of the SEV process for the conk out GPS satellite detection**

series relative to the filter values is obtained as

$$C(k, P) = \frac{1}{N_2}\sum_{i=1}^{N_2}[y_{2,i} - f^{'}(x_{2,i})]^2 \qquad (10)$$

where P is a random division of the even series. $(x_{2,i}, y_{2,i})$, $i = 1, 2, \ldots N_2$ is the validation samples, and $f'(x_{2,i})$ are extracted by cubic spline interpolation of the filter values for the $x_{2,i}$ epoch.

Step 3: Using the decomposed signals between the k_1th and k_2th levels as the filtered values and repeating 'Step 2'. Here the details are from *1* to K levels, and the approximation is presented by the $(K+1)$th level. After that, values of the filter from the k_1th to the k_2th levels is sampled randomly for M times, denoted by P_j, $j = 1,2, \ldots M$. Therefore, equation (11) helps to obtain M variances $C(k_{1,2},P_j)$ and finally, their average can be calculated by

$$\bar{C}(K_{1,2}, P) = \frac{1}{M}\sum_{j=1}^{M} C(k_{1,2}, P_j) \qquad (11)$$

The $k_{1,2}$ is referred to the signal levels of the filtering series. This makes the smallest $\bar{C}(K_{1,2}, P)$.

Step 4: Decomposing the raw observational data series with a $(K+1)$ level WT, and then selecting results from $k_1 + 1$ to $k_2 + 1$ levels based on the 'Step 3' outcomes. Since the sampling rate in the odd series is half of the raw observational series, *a* $(K+1)$ level WT is selected.

Step 5: Saving the coefficients of the signal levels specified in 'Step 4', and then setting the coefficients of the other decomposition levels to zero. Based on the resulted wavelet coefficients, the values filtered from observational series are recreated.

Filter design for the dual-tree CWT

The Dual-Tree CWT (DTCWT) is a relatively recent enhancement to DWT, with additional properties. The only cost is an acceptable redundancy, which is 2^d for signals with d-dimensional. Like designing the filter of real WTs, different approaches exist to the filter's design of the DTCWT, which satisfy the wanted features: approximate half-sample delay, PR biorthogonal or orthogonal, finite support (Finite Impulse Response (FIR) filters), analyticity and linear-phase filters (Sivaramakrishnan and Nguyen 2001). A straightforward approach towards an invertible analytic CWT splits each output of the FB into its positive and negative frequency components using a complex PR FB.

$$\begin{aligned} h_p(n) &= j^n h_0(n), \\ h_n(n) &= j^n h_1(n) \end{aligned} \qquad (12)$$

$h_p(n)$ and $h_n(n)$ follow $h_0(n)$ and $h_1(n)$ in the case of satisfying the PR conditions. Utilising z-transforms, the filter chain generating the wavelet coefficients at the first level as top panel in Fig. 4, which is equivalent to down panel in Figure.

Thus, for this channel the frequency response can be presented as

$$H_{\text{tot}}(z) = H_1(z)H_n(z^2) \qquad (13)$$

Based on this theory, DTCWT uses two real DWTs; the real part of the transform is obtained from the first one and the imaginary part from the second. Both of them satisfy the PR conditions. $g_0(n)$, $g_1(n)$ are the low/high-pass filters of the lower FB, and $h_0(n)$, $h_1(n)$ are the low/high-pass filters of the upper FB. $\psi_h(t)$ and $\psi_g(t)$ denote the two real wavelets in the manner that the complex wavelet $\psi(t) = \psi_h(t) + j\psi_g(t)$ is approximately analytic and supported on only one-half of the frequency axis. Note that the filters are themselves real; no complex arithmetic is needed to implement the DTCWT. They can be executed simply utilising DWT hardware and software since there is no data flow between the two real DWTs, (Selesnick 2004). The implemented approach can be simplified as:

Step 1: Transform the measurement residuals (input signal) to the wavelet domain.

Step 2: Repeat 'Step 1' K (K-level) times to decompose all the wavelet coefficients.

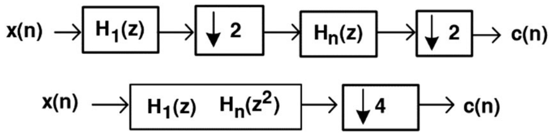
Step 3: Use the specified threshold to eliminate the interference.

Step 4: Invert the wavelet coefficients to the signal domain using inverse transform.

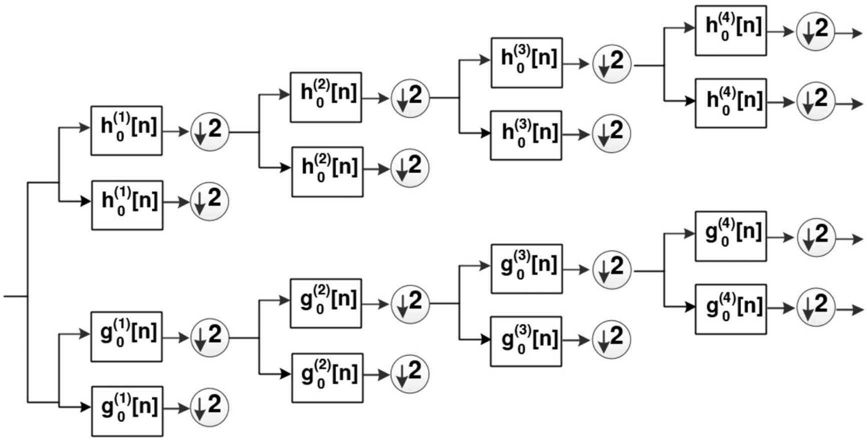
Here, we used

$$\begin{aligned} h_0(n) &= s(n)*d(n), \\ g_0(n) &= s(n)*d(L-n) \end{aligned} \qquad (14)$$

where $*$ denotes discrete-time convolution, and $d(n)$ is



4 **Filter chain in Z domain (top) and equivalent form (bottom)**



5 Proposed FB for the DTCWT with a different set of filters at each stage

supported on $0 \leq n \leq L$.Therefore,

$$H_0(z) = S(z)D(z),\qquad G_0(z) = S(z)Z^L D(1/z) \tag{15}$$

$$|G_0(e^{jw})| = |H_0(e^{jw})|,\qquad \angle G_0(e^{jw}) = \angle H_0(e^{iw}) - 0.5w \tag{16}$$

The later equation presents requirements for the half-sample delay property. The magnitude part of the condition is precisely satisfied, while the phase part is not. From equation (16), we have

$$G_0(z) = H_0(z)A(z) \tag{17}$$

$$A(z) = \frac{Z^{-L}D(1/z)}{D(z)} \tag{18}$$

$A(z)$ is an all-pass transfer function;$|A_0(e^{jw})| = 1$. Therefore,

$$|G_0(e^{jw})| = |H_0(e^{jw})|\qquad \angle G_0(e^{jw}) = \angle H_0(e^{iw}) + \angle A(e^{iw}) \tag{19}$$

In order to satisfy the phase condition approximately by the filters $h_0(n)$ and $g_0(n)$, $D(z)$ should be selected as

$$\angle A(e^{iw}) \approx -0.5w \tag{20}$$

$$D(z) = 1 + \sum_{n=1}^{L} \binom{L}{n} \left[\prod_{k=0}^{n-1} \frac{\tau - L + K}{\tau + 1 + k} \right] (-z)^{-n} \tag{21}$$

In this way, filters are designed in two stages. Introducing a FIR $D(z)$ so that $A(z)$ satisfies equation (20) and then finding a FIR $F(z)$ while $h_0(n)$ and $g_0(n)$ satisfy the PR conditions. This requires only a solution to a linear system of equations and a spectral factorisation.

Implementation issues

Implementing the DTCWT needs that the first stage of the dual-tree FB and the succeeding be different (Fig. 5) (Sivaramakrishnan and Nguyen 2001).

Instead of using the same filters at each stage of the dual-tree FB, we use a different set of PR filters at each stage. The low-pass filters used at stage j are denoted by $h_0^{(j)}(n)$ and $g_0^{(j)}(n)$. Low-pass output of the upper FB at stage j from the input of the FB is dedicated in Fig. 6. $h_{tot}^{(j)}(n)$ is given by

$$H_{\text{tot}}^{(j)}(z) = H_0^{(1)}(Z)H_0^{(2)}(z^2)\dots H_0^{(j)}(Z^{2j-1}) \tag{22}$$

We have a similar expression for $g_{\text{tot}}^{(j)}(z)$ in the lower FB. To make sure that the functions of discrete analysis of the DTCWT meet the interlacing condition, it is required that

$$\begin{aligned} &\text{stage 1:} g_{\text{tot}}^{(1)}(n) \approx h_{\text{tot}}^{(1)}(n-1)\\ &\text{stage 2:} g_{\text{tot}}^{(2)}(n) \approx h_{\text{tot}}^{(2)}(n-2)\\ &\text{stage 3:} g_{\text{tot}}^{(3)}(n) \approx h_{\text{tot}}^{(3)}(n-4) \end{aligned} \tag{23}$$

Equivalently in the frequency domain:

$$\begin{aligned} G_0^{(1)}(e^{jw}) &\approx e^{-jw} h_0^{(1)}(e^{jw})\\ G_0^{(2)}(e^{jw}) &\approx e^{-j0.5w} h_0^{(2)}(e^{jw})\\ G_0^{(3)}(e^{jw}) &\approx e^{-j0.5w} h_0^{(3)}(e^{jw}) \end{aligned} \tag{24}$$

By turning that for every step, $j > 1$, evermore the same condition can be obtained:

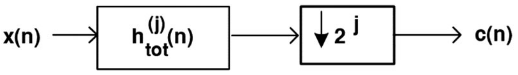
$$g_0^{(j)}(n) \approx h_0^{(j)}(n - 0.5) \tag{25}$$

Only the first level needs a various filter set. Besides, any PR filters can be utilised for the first level. However, it is needed to offset them by one sample from each other.

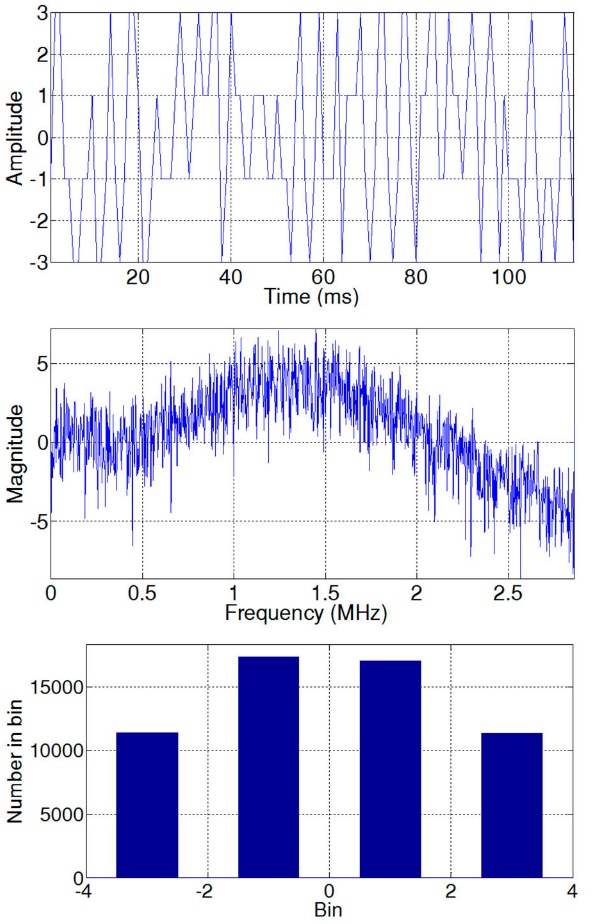
Test data

In this section, we discuss the simulation analysis. Several datasets were investigated, and all results reduced the effect of spoofing in the receiver. In the intermediate spoofing, the 'bogus' receiver could be placed in the adjacency of target receiver. Indeed, it would track, modify, and retransmit the signals being received from the GPS satellites (Baziar *et al.* 2015).

We managed to use existing published research and open source code available to program a Software Defined Receiver (SDR) that would work as a GPS emulator (Borre *et al.* 2007). There are two parts of the

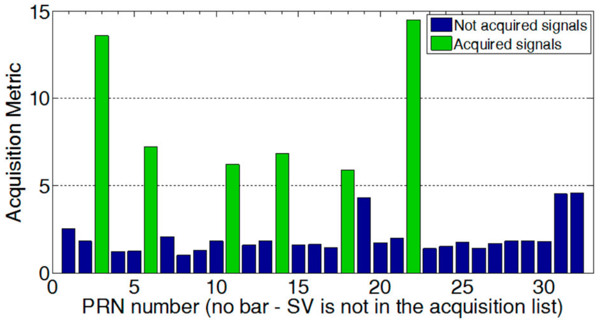


6 Low-pass output of the upper FB at stage *j*



7 Raw data information. Time domain (top), frequency domain (middle), and histogram (bottom)

position fix solution. One is accuracy or the distance between the computed solution and the actual position, and the other is integrity, or the confidence that the computed solution is right. With only four satellites in view, the accuracy is high, but the integrity is poor. With 16



8 Acquisition results of a sample GPS data in SDR

LOS satellites, the accuracy may be poor, but the integrity is high. Therefore, a proper trade-off is needed for selecting the optimised number of LOS satellites.

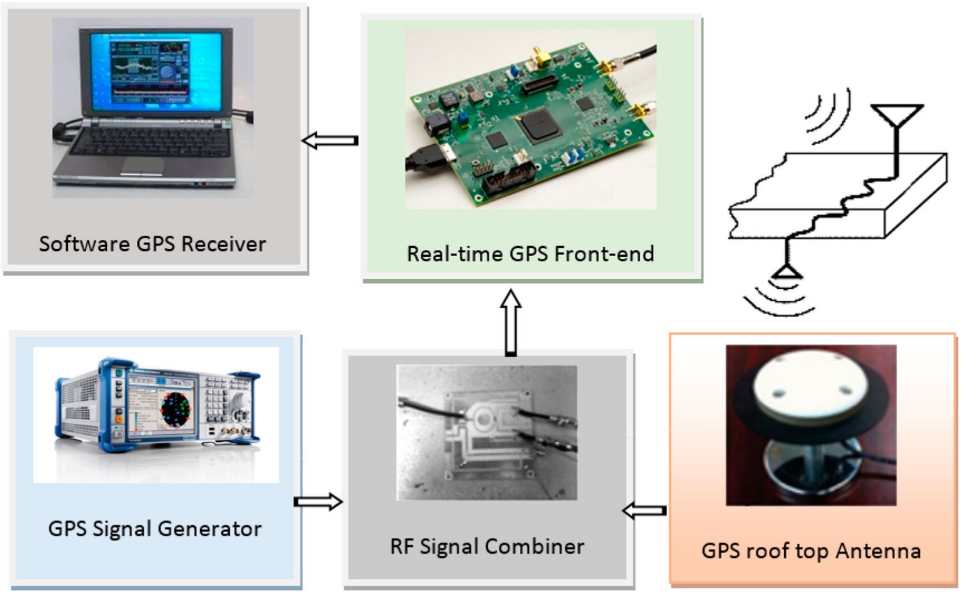
Processing of proposed methods is done by a SDR in a single-frequency approach. Figs. 7 and 8 have been related to results of the raw data information and visible satellites in the acquisition, respectively.

Top panel in Fig. 7 shows time-domain plot of 2-bit four level data. Middle panel shows frequency domain of signal. The maximum amplitude of signal is seen at 1.4 MHz. The bottom panel shows the histogram of four levels if the GPS signal.

Fig. 8 shows the number of visible satellites. Green colour shows detected satellites. At least four satellites are required for the receiver to compute navigation solution or PVT. Here, six satellites are visible. Laboratory platform scheme of the total system is demonstrated in Fig. 9. We now define GPS spoofing attack and analyse how our attacker can spoof the locations of GPS receivers.

Stationary simulated data set

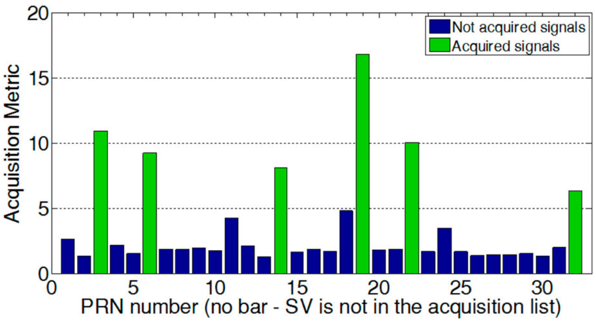
Spoofer-receiver holds back original signal (x_k) to generate a counterfeit signal. A mixture of the delayed and original signal reaches the GPS receiver. In fact, the received signal is the sum of the original and spoofing signal in the target receiver. The following equation shows



9 Top level model for implemented system

Table 1 Details of stationary spoofing data sets

	Simulated (m)				Measurement (m)			
Spoofing data sets	ΔE	ΔN	ΔU	RMS	ΔE	ΔN	ΔU	RMS
Low position error	13	39	57	70	9	73	81	109
	12	53	110	123	16	47	103	114
	8	44	213	218	28	48	104	118
Middle position error	9	76	343	351	26	112	87	144
	10	88	392	402	6	103	166	195
	133	153	473	515	18	125	199	236
High position error	210	237	745	810	59	310	265	412
	233	264	829	901	324	266	242	484
	309	341	1092	1185	314	204	382	535



10 Acquisition result of the spoofed data

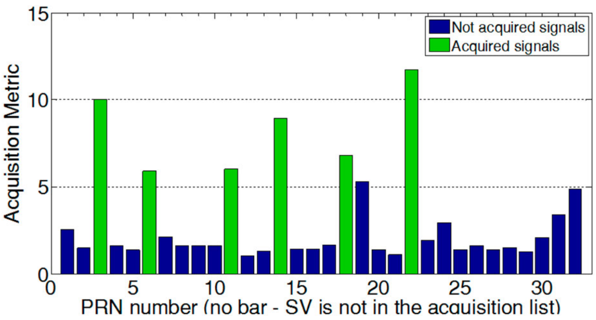
the received signal in the GPS receiver after spoofing. In this equation, y_k is known as the spoofing signal.

$$y_k = x_k + a x_{k-d} \tag{26}$$

where the coefficient $\alpha > 1$ is amplitude advantage factor of the delayed signal and $d > 0$ is the number of samples of spoofing delay (Baziar *et al.* 2015). Because the power of the spoofing signal to be more than the original signal, it is multiplied by a greater number than one.

Stationary measurement data set

In the second data set, we tried to deliverance from quantisation error due to the A/D in the front-end module. For this purpose, we decided to combine the RF signals instead of IF signals. With regard to our laboratory equipment, this can be feasible only with a GPS signal simulator. It is generally assumed that output of simulator is much the same signal directly taken from the GPS antenna. The resulting signal is applied to a front-end that makes ready the proper two-bit digital signal for SDR.



11 Acquisition result of the modified data

Table 1 lists some examples of each group and specifies the position error in East, North, and Up (ENU) coordinates. Root Mean Square (RMS) refer to the position difference between navigational solutions based on authentic and spoof signals. ΔU is the height difference. ΔE and ΔN are varied in surface horizons. Low position error includes positioning error less than 300 m. Spoofing between 300–500 m called intermediate spoofing. Errors higher than 500 m are considered as high position error.

Semi-dynamic measurement data set

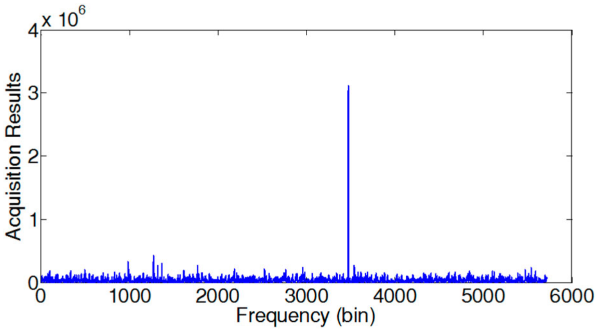
In order to test the proposed approach in a more realistic condition, dynamic delay spoofing is also generated as the 3rd data set. In this case, the authentic signal relates to a moving car with constant speed and attacker sends GPS signals of its position toward the target receiver. In other words, target receiver is moving but the spoofer is static.

Dynamic simulated data set

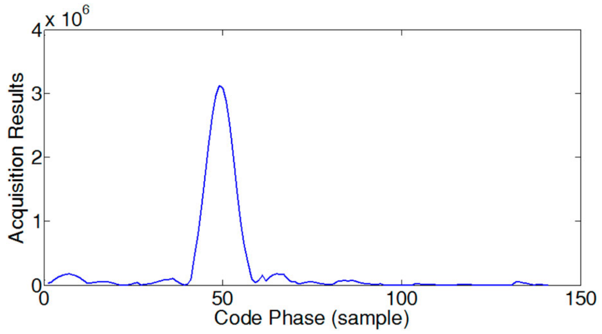
Finally, in the most real case, both of authentic and counterfeit signals are dynamic. The target receiver is moving in right raw but spoofer tries to deviate that in the middle of the route. All processing was done on a laptop ASUS K46C with i5 1.8 GHz CPU.

Test results

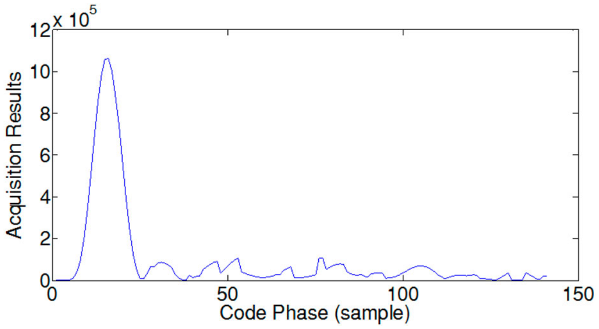
We present simulation results of the proposed method on all data sets here. Fig. 10 shows acquisition results for the spoofed version of sample data demonstrated in Fig. 8. As



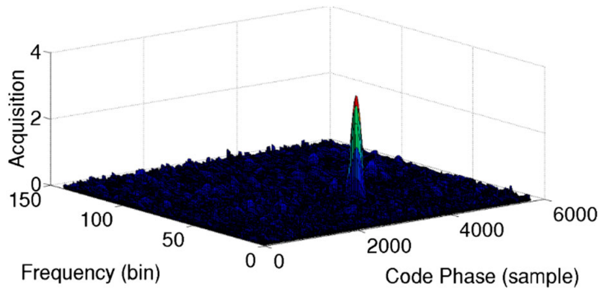
12 Acquisition result of PRN11 versus code phase (authentic signal)



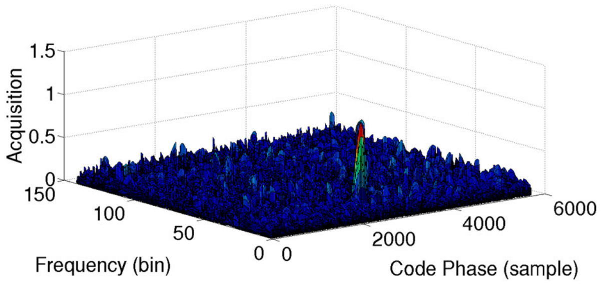
13 Acquisition result of PRN11 versus frequency bin (authentic signal)



16 Acquisition result of PRN11 versus frequency bin (weak signal)



14 Acquisition result of PRN11 (authentic signal)



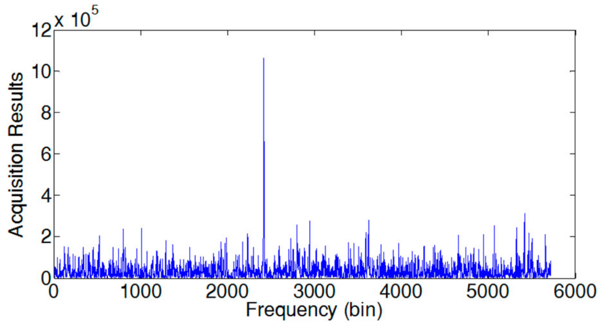
17 Acquisition result of PRN11 (weak signal)

can be seen, six satellites are visible. The simulation is configured that each green satellite is not valid satellite. Rather only four satellites are authentic actually. As shown in Fig. 8, PRNs 3, 6, 11, 14, 18 and 22 are visible in authentic signal and according to Fig. 10, PRNs 3, 6, 14, 18, 19, 22 and 32 are visible after applying spoof attack. Therefore, the attack causes that PRNs 11 and 18 be invisible in acquisition stage and two counterfeits be injected. In addition, PRNs 19 and 32 are included in acquired satellite during the spoof attack but after applying Fake Satellites Identification (FSI) algorithm, they are not considered. Moreover, PRNs 11 and 18 are detected through SEV algorithm (Fig. 11).

In Figs. 12–17, we will analyse the results of the attack on acquisition results of PRN 11. Fig. 12 shows acquisition result of PRN11 versus code phase in authentic signal. The peak of acquisition correlation function is at the sample 3450. Acquisition result of PRN11 in authentic signal versus frequency bin is demonstrated in Fig. 13. Here, the peak of acquisition correlation function is at the sample 50. Information of both figures can be seen in Fig. 14 in 2-demantional plot. Fig. 15 shows acquisition result of PRN11 versus code phase in spoofed signal. Acquisition result of PRN11 in spoofed signal versus frequency bin is demonstrated in Fig. 16. The peak of acquisition correlation function occurs at the same samples of authentic signal with about 10 times lower power due to spoofing. Information of both figures can be seen in Fig. 17 in 2-demantional plot. It is evident from the figures that of the signal power of satellites decrease under spoof condition.

The following experiments demonstrate the significant improvements. The SEV and FSI processes help the SDR to detect the low power GPS satellites and ignore fake PRNs.

During acquisition process in SDR, correlation results are calculated in frequency steps of 0.5 kHz. After that, a maximum correlation value is determined as the peak. The second highest correlation peak in the frequency bin of the highest peak is found. The ratio of these two peaks named as correlation peak to next peak ratio (CPPR) is compared to the value preset in the receiver variable *acq_threshold* by default amount of 5.8. In other words, the satellites with CPPR more than 5.8 were recognised. Acquired satellites information of three



15 Acquisition result of PRN11 versus code phase (weak signal)

Table 2 Acquired satellites information of authentic GPS data

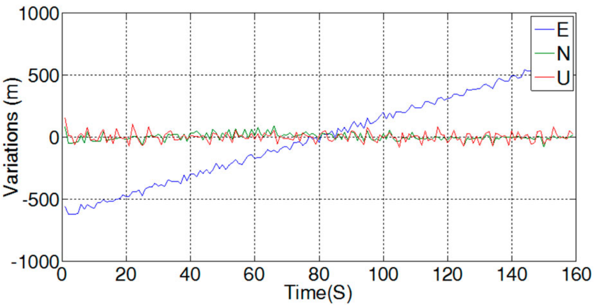
PRN	Code phase sample	Frequency bin index	CPPR (dB)
3	5034	71	12.4
6	2322	74	6.5
11	2384	16	6.9
14	1013	47	6.3
18	778	69	6.7
22	326	58	10.3

Table 3 Acquired satellites information of spoofed GPS data

PRN	Code phase sample	Frequency bin index	CPPR (dB)
3	5034	71	10.5
6	2322	73	6.8
14	1016	48	14
19	1959	50	14.3
22	328	58	10
32	889	23	7.3

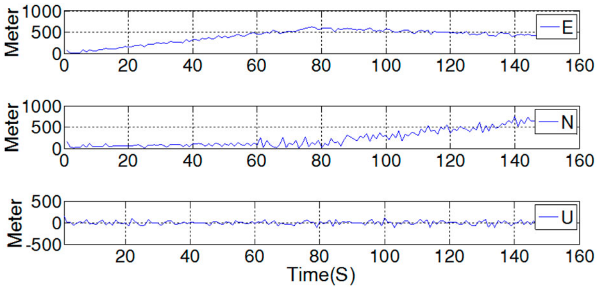
Table 4 Acquired satellites information of modified GPS data

PRN	Code phase sample	Frequency bin index	CPPR (dB)
3	5033	70	7.9
6	2330	74	6.4
11	2239	16	6.2
14	950	48	8.5
18	773	69	5.9
22	1643	22	7.8



18 Position results of semi-dynamic data

discussed data sets is listed in Tables 2–4 including the code delay samples, the carrier frequency, the PRNs and the estimated CPPRs. It is worst to note that each PRNs in all of three data sets are located at the similar carrier frequency and code phase but not the same exactly.



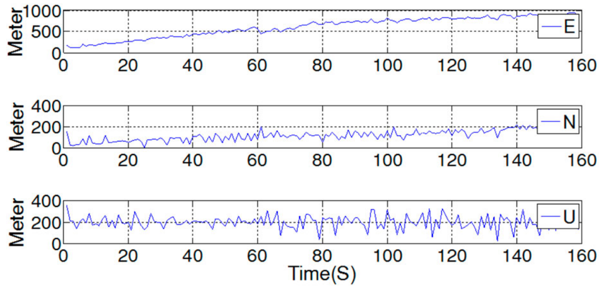
19 Position results of semi-dynamic spoofed data

Table 2 shows the acquisition results of the collected authentic signal. Table 3 shows the acquisition results of the spoofed signal. Spoofing changes the CPPR ratio of common PRNs, 3, 6, 14, 22. The attenuation is expectable for a satellite signal with a low received power. As shown in Table 4, after applying the proposed algorithm CPPR ratio change toward their initial value. In reality, the satellite signals of PRNs 11 and 18 are LOS, as shown in Table 2. The SEV process also confirmed that they are present. The suggested SEV method is performed on the other signals of satellite, which were previously declared as signal absent in Table 4. Therewith, two PRNs, which do not exist in Table 3, are now declared as signal present.

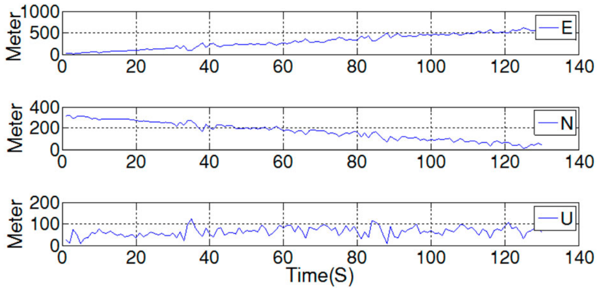
Table 5 demonstrates countermeasure results for simulated and measurement stationary data sets. Here, RMS refers to displacement between navigational solutions based on spoof and authentic signals, ΔEN is displacement in the earth and ΔH is the height difference. For instance, the last raw in the table refers to a data set with 535 m spoofing error which decreased to 38 m after performing SEV and FSI methods in acquisition. In more detail, ΔH is reduced from 382 to 25 m and ΔEN from 374 to 28 m. Generally, the anti-spoofing approach reduced the simulated spoofing error in average of 86%, with a tolerance of 11%. Likewise, in measurement data impact of attack diminished in an average of 83%, with a tolerance of 32%. It is worth to note that tolerance for

Table 5 Error reductions using proposed approach

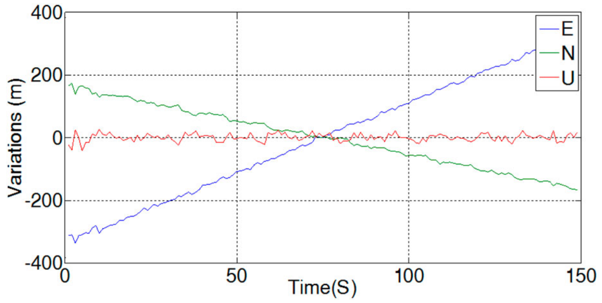
	Before reduction (m)			After reduction (m)			
Interference	RMS	ΔH	ΔEN	RMS	ΔH	ΔEN	Error reduction %
Simulated	70	57	40	10.5	7	7.8	85
	123	110	55	23	17	15	81
	218	213	46	24	21	12	89
	351	343	83	63	54	32	82
	402	392	90	76	59	48	81
	515	473	204	57	43	37	89
	810	745	318	146	120	83	82
	901	829	353	72	55	46	92
	1185	1092	460	94	81	49	92
Measurement	109	81	73	38	31	22	65
	114	103	49	36	24	27	68
	118	104	56	22	13	18	81
	144	87	115	10	6	8	93
	195	166	102	21	17	13	89
	236	199	127	52	44	28	78
	412	265	315	50	42	26	88
	484	242	419	53	39	36	89
	535	382	374	38	25	28	93



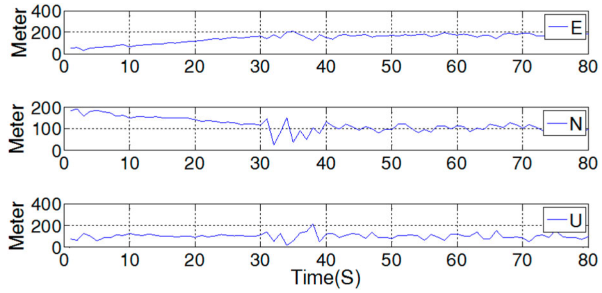
20 Position results of semi-dynamic modified data



23 Position results of dynamic modified data



21 Position results of dynamic data



22 Position results of dynamic spoofed data

each spoofing data is the divergence between the lowest and highest spoofing mitigation percentage.

The results of simulations for dynamic data sets are shown in Figs. 18–23, obtained in Universal Transverse Mercator (UTM) system. Figs. 18 and 21 show position results of semi-dynamic and dynamic data sets, respectively. As shown in Fig. 18, in semi-dynamic data only *E* coordinate changes with time. In dynamic data both of *E* and *N* coordinates are changing. As can be seen in Fig. 19, spoofing attack starts in 80 seconds. The attack stops variations of *E* coordinates and causes fake variations in *N* coordinate. In addition, the noise of *U* coordinates increases slightly due to spoofing. Fig. 20 shows position results after applying the anti-spoofing method. As can be seen, variations of all three coordinated are close to authentic one.

Fig. 22 shows coordinate variations of spoofed dynamic data. Variations of *E* and *N* coordinates are stopped due to spoofing. After applying the proposed approach, position results return to the initial authentic state largely. The performance of this method is almost 78% interference reduction on the simulated dataset and 87% 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.

Another important result was achieved. After the navigation solution processing, *Position Dilution of Precision* (PDOP) parameter is significantly reduced and improved. The GPS receiver let the display of its position and the PDOP value. PDOP is given as discrete measurements in 3D position. It follows mathematically the positions of the operative satellites. Low values of the PDOP parameter indicates a better positioning precision because the wider angular separation between the satellites used to compute a position.

Table 6 Comparing previous methods and proposed algorithm

Detection methods	Analysed features	Required equipment	Advantages	Limitations	Total mark
SQM	Correlation branch (5)	Software upgrade (6)	Easy detection (5)	Inefficient in synchronous attacks, 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
VB	Correlation branch (3)	Additional tracking loop (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
This work	IF signal (5)	Software upgrade (6)	Easy to implement, real-time and reliable (9)	Algorithm needs prior data (5)	21

Table 6 presents properties discussed in Section 1 and suggested algorithm on the examined factors, required equipment, limitations and advantage approaches. In order to have a better judgment, a numerical value was assigned to each feature. The worst and the best cases are considered for any feature; score 0 is dedicated to the worst state and score 10 is devoted to the best state. After that, depending on the algorithm performance a number from 0 to 10 is assigned to any feature. For example, the feature 'necessary equipment', an algorithm takes 10, if no extra equipment is needed. Besides, in the case of necessity to basal changes in receiver structure, it earns 0. As can be seen, the proposed algorithm performs better than others do because the offered method needs no extra hardware and does not increase the receiver size and the production costs.

Conclusions

In this study, we focused on spoofing threat as an important disturbance. The investigated approach is implemented based on a redundant type of CWT, the dual-tree approach, which is based on two FB trees. First, fake satellites are identified using CWT thresholding, on which external disturbances are presented in the form of high wavelet coefficients. After omission of fake satellites, SEV process tries to identify the conk out satellites due to spoofing. Cross-validation technique is used for automatically identifying wavelet signal layers. Previous techniques have high implementation costs, because of adding extra hardware, may need some changes to be made in the GPS receiver operation. However, the suggested technique requires no additional hardware and have a simple implementation with little modification at acquisition level. The suggested algorithm has been tested on four interference data sets. The simulation results are good to prove the effectiveness of the CWT based method to mitigate the interference.

References

Ahmad, S.F., Sasibhushana Rao, G., and Ganesh, L., 2016. A robust GPS signal acquisition technique using discrete wavelet transform. *Procedia computer science*, 85, 683–690.

Arlot, S., and Celisse, A., 2010. A survey of cross-validation procedures for model selection. *Statistics surveys*, 4, 40–79.

Azarbad, M.R., and Mosavi, M.R., 2014. A new method to mitigate multipath error in single-frequency GPS receiver based on wavelet transform. *GPS solutions*, 18 (2), 189–198.

Baziar, A.R., Moazedi, M., and Mosavi, M.R., 2015. Analysis of single frequency GPS receiver under delay and combining spoofing algorithm. *Wireless personal communications*, 83 (3), 1955–1970.

Bonebrake, C., and O'Neil, L.R., 2014. Attacks on GPS time reliability. *IEEE Transactions on security & privacy*, 12 (3), 82–84.

Borre, K., *et al.*, 2007. *A software-defined GPS and Galileo receiver: a single-frequency approach*. Boston, MA: Birkhäuser.

Chien, Y.R., 2018. Wavelet-packet-transform-based anti-jamming scheme with new threshold selection algorithm for GPS receivers. *Journal of the Chinese institute of engineers*, 41 (3), 181–185.

Chien, Y.P., Chien, P.Y., and Fang, S.H., 2017. Novel anti-jamming algorithm for GNSS receivers using wavelet-packet-transform-based adaptive predictors. *IEICE Transactions on fundamentals of electronics, communications and computer sciences*, E100-A (2), 602–610.

Collin, F., and Warnant, R., 1995. Applications of the wavelet transform for GPS cycle slip correction and comparison with Kalman Filter. *Manuscripta geodaetica*, 20, 161–172.

Fu, W.X., and Rizos, C. 1997. The applications of wavelets to GPS signal processing. *10th international technical meeting of the satellite division of the U.S. Institute of Navigation*, Kansas City, Missouri, 1385–1388.

Jahromi, A.J., *et al.*, 2012a. GPS Spoofer countermeasure effectiveness based on signal strength, noise power, and C/N0 measurements. *International journal of satellite communications and networking*, 30 (4), 181–191.

Jahromi, A.J., *et al.*, 2012b. GPS vulnerability to spoofing threats and a review of anti-spoofing techniques. *International journal of navigation and observation*, 2012, 1–16.

Jwo, D.J., and Lai, C.N., 2008. Unscented Kalman filter with nonlinear dynamic process modeling for GPS navigation. *GPS solutions*, 12, 249–260.

Kaplan, E., and Hegarty, C.J., 2007. *Understanding GPS: principles and applications*. 2nd ed. Norwood, MA: Artech House.

Kingsbury, N.G., 2001. Complex wavelets for shift invariant analysis and filtering of signals. *Applied and Computational harmonic analysis*, 10 (3), 234–253.

Kwon, K.C., Yang, C.K., and Shim, D.S., 2014. Spoofing signal detection using accelerometers in IMU and GPS information. *The transactions of the Korean institute of electrical engineers*, 63 (9), 1273–1280.

Lawrence, L., 2017. Wavelet packets based denoising method for measurement domain repeat-time multipath filtering in GPS static high-precision positioning. *GPS solutions*, 21 (2), 461–474.

Ledvina, B.M., *et al*. 2010. An in-line anti-spoofing device for legacy civil GPS receivers. *ION GNSS 2010*, 25–27 January, San Diego, CA: Institute of Navigation, 689–712.

Mosavi, M.R., and Emamgholipour, I. 2013. De-noising of GPS receivers positioning data using wavelet transform and bilateral filtering. *Journal of Wireless Personal Communications*, 71 (3), 2295–2312.

Mosavi, M.R., Nasrpooya, Z., and Moazedi, M., 2016. Advanced anti-spoofing methods in tracking loop. *Journal of navigation*, 69 (4), 883–904.

Mosavi, M.R., and Shafiee, F., 2016. Narrowband interference suppression for GPS navigation using neural networks. *GPS solutions*, 20 (3), 341–351.

Motella, A.B., Pini, M., and Fantino, M. 2010. *Detection of spoofed GPS signals at code and carrier tracking level*. 5th ESA workshop on satellite navigation technologies and European workshop on GNSS signals and signal processing, Noordwijk, Netherlands, 1–6.

Mitelman, A.M. 2004. *Signal quality monitoring for GPS augmentation systems*. Thesis (PhD). Stanford University.

Ogaja, C., *et al*. 2001. *Towards the implementation of on-line structural monitoring using RTK-GPS and analysis of results using the wavelet transform. 10th FIG International Symposium on Deformation Observations,* California, USA, 284–293.

Satirapod, C., Wang, J., and Rizos, C., 2003. Comparing different GPS data processing techniques for modelling residual systematic errors. *Journal of surveying engineering*, 129 (4), 129–135.

Selesnick, I.W., 2004. The double-density dual-tree discrete wavelet transform. *IEEE transactions on signal processing*, 52 (5), 1304–1314.

Sivaramakrishnan, K., and Nguyen, T., 2001. A uniform transform domain video codec based on dual tree complex wavelet transform. *IEEE international conference acoustic, speech, signal processing*, 3, 1821–1824.

Warner, J.S., and Johnston, R.G., 2002. A simple demonstration that the global positioning system (GPS) is vulnerable to spoofing. *Journal of security administration*, 25 (2), 19–27.

Wesson, K.D., *et al*. 2011. An evaluation of the vestigial signal defense for civil GPS anti-spoofing. *ION GNSS 2010*, 20–23 September Portland, OR: Institute of Navigation, 2646–2656.

Zhong, P., *et al.*, 2008. Adaptive wavelet transform based on cross-validation method and its application to GPS multipath mitigation. *GPS solutions*, 12, 109–117.