JAST, Vol. 10, No. 2, pp. 9- 16
© Iranian Aerospace Society, Summer-Fall 2013

A Wavelet-based Spoofing Error Compensation Technique for Single Frequency GPS Stationary Receiver

A. R. Baziar[1], M. Moazedi[2], M. R. Mosavi[3*]

1, 2, 3. Department of Electrical Engineering, Iran University of Science and Technology
[*]Postal Code: 16846-13114, Tehran, IRAN
m_mosavi@iust.ac.ir

Spoofing could pose a major threat to Global Positioning System (GPS) navigation, so the GPS users have to gain an in-depth understanding of GPS spoofing. Since spoofing attack can influence position results, spoof compensation is possible through reducing position deviations. In this paper, a novel processing technique is proposed and the wavelet transform is used to eliminate the impact of spoofing on the stationary GPS receivers. We assumed that the spoofing attack was immediately detected, and then the position residuals of the last authentic and new spoofing signals were passed to the statistic wavelet transform at the first level. By denoising in the next step, position deviations due to the spoofing attack can be extracted. Then, the estimated position solution of the received signal is corrected. Finally, the receiver coordinates are calculated by averaging the corrected positions. For validation of the suggested algorithm, five different data sets are investigated. We mitigated the spoofing in all data sets more than 93%. The test results show that the proposed technique supremely improves the performance of the GPS receiver and attenuates the spoofing effect.

Keywords: GPS Spoofing, Statistic Wavelet Transform, Single Frequency Receiver, Anti-Spoofing.

Symbols and acronyms

GPS	Global Positioning System
RF	Radio Frequency
SQM	Signal Quality Monitor
VSD	Vestigial Signal Defense
VB	Vector Based
FT	Fourier Transform
WT	Wavelet Transform
CWT	Continuous Wavelet Transform
DWT	Discrete Wavelet Transform
$\psi(t)$	Mother Wavelet

Introduction

Global Positioning System (GPS) is an impressive and important navigational tool. Over the past two decades, security and reliability of GPS-based systems have been restricted (Mosavi, 2006). The GPS is extremely vulnerable to different kinds of interference. This makes GPS spoofing one of the important research topics (Humphreys et al., 2008). Spoofing tells vehicle operators (or, theoretically, smartphone users) a false location.

Spoofing attacks can be classified into three main groups: simplistic, intermediate and sophisticated. Simplistic attackers attach a power amplifier and an antenna to a GPS signal simulator and radiate the Radio Frequency (RF) signal toward the target receiver. These signals are not aligned with the current broadcast GPS signals. However, if the adversary can transmit signals with a power higher than the legitimate signal, misleading commercial receivers would be possible (Jahromi et al., 2012a).

The second group synchronizes its counterfeit GPS signals with the authentic GPS signals, so that the fake signals can more-easily masquerade as genuine ones. The receiver-spoofer can be formed small enough to

[1] M.Sc.
[2] PhD Graduate
[3] Professor (Corresponding Author)

be placed indistinctly near the antenna of the victim receiver. The receiver-spoofer could even be located far away from the target if the it was stationary, or its position can be estimated relative to the attacker.

Sophisticated attacks include several receiver-spoofers using a common reference oscillator and communication link and each one is adjusted to the one target antenna. Implementation of these attackers is so hard and impossible in some cases because of the target receiver motion (Jin et al, 2011).

The first step to counter the spoofing attack is detection of attack, and the next step is to compensate its effect (Humphreys et al, 2010). During the past decade, several algorithms have been developed and tested for interference detection and mitigation (Jahromi et. al., 2012a). This paper presents an anti-spoofing technique to reduce the spoofing error after the uncovering of the attacks. The rest of this paper is organized as follows. Firstly, we will have a short review of spoofing mitigation approaches. Section 3 introduces Wavelet Transform (WT) and its application in GPS signal processing. The proposed algorithm based on WT is described in section 4. Section 5 relates simulations and test results for investigating the suggested technique. Finally, section 6 states the conclusion and its comparison with earlier works.

Prior Works on GPS Spoofing Mitigation

A part of anti-spoofing methods, considered in the primary studies of this field, is based on constantly investigating and comparing the internal and external information and estimating the authentic signal (Jin et al., 2011; Lin et al., 2007; Papadimitratos & Jovanovic, 2008). In Ref. (Papadimitratos & Jovanovic, 2008), the receiver has two operation modes. In the normal mode, the receiver relies on the collected information and compares the predicted values with the obtained position-velocity-time solutions in alert mode. If those positions match the suspected and duplicitous ones, the receiver returns to its normal mode. The location prediction in this system is implemented by Kalman filtering or inertial sensors.

By reason of practical limitations, spoofers, except sophisticated ones, often transmit several counterfeit signals from a single source, while the authentic signals are broadcasted from different satellites and directions. Thus, spatial processing can be used to estimate the three-dimensional effects of the received signals and spatially separate the correlated ones (McDowell, 2007; Daneshmand et al., 2011; Daneshmand et al., 2013; Nielsen et al., 2010). The basic assumption is that if more than one counterfeit signal is transmitted from a common source, signal array manifold vectors are spatially correlated. Then, the attacker existence is likely.

Another technique, called Receiver Autonomous Integrity Monitoring (RAIM), has been proposed for detecting and mitigating spoofing threat at navigation and position solution level (Ledvina et al., 2010). This method detects damaged pseudo-ranges and excludes the measurement errors from navigation solution via statistical hypothesis testing. Moreover, signal monitoring techniques are applied to detect spoofing attacks on tracking receivers. During a spoofing attack, the receiver should be able to extract the authentic signal. For this purpose, Vector Based (VB) tracking structures have been employed. The basic idea in this technique is combining the navigation solution and the signal tracking burdens in order to increase the robustness of GPS receivers against the interference (Jahromi et al., 2012b).

Signal Quality Monitor (SQM) is related to proper algorithms so as to be implemented within the GPS receivers and to be able to continuously observe received GPS signals for interference, distortion, and other anomalies with the purpose of raising a warning flag. SQM methods can effectively detect the fake correlation peak approaching the authentic signal. However, they are inapplicable where spoofing attack does not affect the correlation shape. This situation happens when counterfeit and authentic signals are almost aligned (Ledvina et al., 2010). To improve the performance in practical situations, several approaches based on SQM are suggested, namely Vestigial Signal Defense (VSD), VB tracking and the combined technique.

The VSD relies on the difficulty of suppressing the true GPS signal during an attack. In other words, this technique monitors anomalies in the complex correlation domain to detect interferences. A significant issue for VSD to overcome is that the interaction of the authentic and fake GPS signals is similar to the interaction of multi-path and line of site GPS signals. Differentiating the two types of interference is a significant challenge for any interference defense based on monitoring the complex correlation domain. The effectiveness of VSD is limited by the difficulty of differentiating spoofing from multi-path (Wesson et al., 2011).

The main idea in VB tracking technique is combining the navigation solution and the signal tracking burdens in order to increase the robustness of GPS receivers against the interference (Jahromi et al., 2012b). It is the analytical approach to investigate the interaction between the authentic and the counterfeit correlation peaks during attacks. Then, an interference detection technique based on amplitude analysis of different correlator branches is proposed, which continuously checks the distribution of each correlator output. Spoofing attack is detected if this distribution considerably deviates from that of the authentic signal.

A VB tracking receiver structure has been also employed to extract the authentic signal during the attack. Another technique, called RAIM, has been proposed for detecting and mitigating integrity threat at the navigation and position solution level (Ledvina et al., 2010). This method detects damaged pseudo-ranges and excludes the measurement errors from navigation solution via statistical hypothesis testing.

The combined technique "sandwiches" an attacker between a correlation function distortion monitor and a total in-band power monitor. The defense exploits the difficulty of mounting an effective attack that simultaneously maintains a low-enough counterfeit signal power to avoid power monitoring alarms while minimizing distortions of the received cross-correlation profile being indicative of an attack.

Wavelet Transform and Its Application in GPS Signal Processing

Currently, WT is used in many mathematical and engineering applications. The advent of this strong tool is considered as the most important occurrence in signal processing after Fourier Transform (FT). Indeed, WT obtains possibility of simultaneously analyzing both time and frequency domains. This transformer demonstrates local information about the signal through dilations and translations of an adaptive window, called a wavelet. The WT applies two simultaneous processes on the wavelet, considered as mother wavelet. This transform can be performed in a continuous or discrete way. If the wavelet coefficients are computed at every possible scales and positions, Continuous Wavelet Transform (CWT) will be performed as:

$$WT(s,\tau) = < \Psi_{s,\tau}, x > = \frac{1}{\sqrt{s}} \int_{-\infty}^{+\infty} \Psi(\frac{t-\tau}{s}) x(t) dt \qquad (1)$$

Where x(t) is the transformed signal, $\psi(t)$ is the mother wavelet, w is the wavelet function, s is the dilation factor, and τ is the translation parameter. Both s and τ are arbitrary scalar values, but s is not zero. Variations of the time and frequency resolutions of the mother wavelet at two locations on the time-frequency plane, (τ_1, η /s$_1$) and (τ_2, η /s$_2$) are demonstrated in Fig.1. An important step in the transformation process is to choose the best mother wavelet. Through a variety of scale and time shifts of the mother wavelet, the WT can take the signal components in its whole spectrum. Small scales are employed to decompose high-frequency parts and large scales for low-frequency components analysis (Chang, 2014) .As computing the wavelet coefficients at every possible scale is a time-consuming process, reconstruction of the original signal in the Discrete Wavelet Transform (DWT) is easier and faster than CWT. Thus, DWT is used mostly for a perfect reconstruction of the original signal. Considering this grid, the DWT can be represented as follows:

$$\psi_{m,n}(t) = a^{-m/2} \psi(a^{-m} t - nb) \qquad (2)$$

$$y(t) = \sum_{m \in Z} \sum_{n \in Z} < y, \Psi_{m,n} >, \Psi_{m,n}(t) \qquad (3)$$

Where integers m and n control the wavelet dilation and translation, respectively.

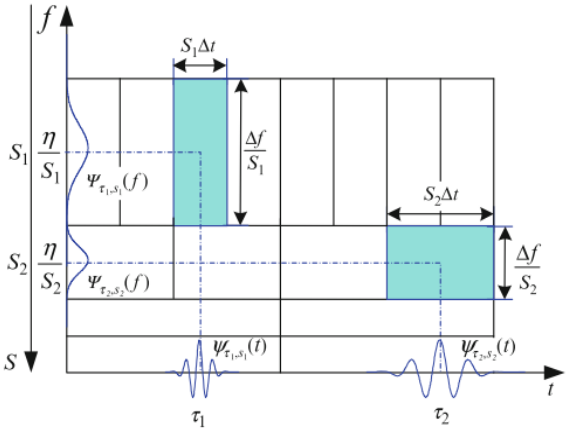

Figure 1. Variations of time and frequency resolutions of the mother wavelet (Chang, 2014).

WT has a wide variety of new and exciting applications such as filtering, sub-band coding, data compression and multi-resolution signal processing. One of the efficient applications of WT in signal processing is studying the non-stationary signals. GPS observations belong to this signal category. It is worth noting that, analyzing these signals by using FT is not possible (Satirapod et al., 2003). Efficiency of spoofing extraction essentially depends on choosing the mother wavelet for the WT. The other important subject is the decomposition level which depends on the sub-band frequency, including the spoof signal (Souza et al., 2008).

Firstly, 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. According to this study, GPS bias terms such as multi-path and ionosphere delay behave like low-frequency noise and the observations behave as high-frequency noise (Fu & Rizos, 1997). Ogaja introduced the WT to analyze the GPS results in a structural monitoring application (Ogaja et al., 2001). Satirapod applied different wavelets to separate the systematic error component from the noise component in the GPS double differenced residuals (Satirapod et al., 2002).

The denoising and feature detection of signals using the WT is done through representing the signal by a small number of coefficients. Denoising attempts to remove whatever noise is present and retain whatever signal is present regardless of the frequency content of the signal. Wavelet shrinkage denoising is considered a non-parametric method, based on thresholding, as developed by Donoho and Johnstone, 1994.

Thresholding generally gives a low-pass version of the primary signal. An appropriate threshold can put out noise of a signal. In fact, noise is usually mounted at finer scales, so the noise will be eliminated by discarding the coefficients lower than a specified threshold at these scales.

Denoising is not limited to a special type of noise. Different denoising approaches can throw away various kinds of interferences from the signals. The signal is composed into L levels before thresholding is applied. There are two types of thresholding, hard and soft. Hard thresholding zeros out small coefficients, resulting in an efficient representation. Soft thresholding decreases coefficients by the threshold value to exceed them for smoothing the signal. Generally, this thresholding is used for denoising applications. It is assumed that the noise power is smaller than the signal power. In other words, the denoising by thresholding removes either a large part of the signal besides the noise or leaves a larger part of the noise in the signal. Generally, it is impossible to completely filter out the noise without harming the initial signal (Merry, 2005). Theoretical foundation for modeling the suggested anti-spoofing algorithm and the spoofing reduction operation in the GPS signal will be described later.

Proposed Method for Spoofing Mitigation

Through analyzing the effect of spoofing in the receiver software, we discovered that spoofing attacks mainly distort the pseudo-range and satellites position. Since the navigation solution and founded GPS coordinates of location are based on these specifications, noticeable differences exist in the estimated position of the GPS receiver relative to its current location. This paper introduces a new method to mitigate spoofing in the single frequency GPS receivers by using WT. The signal parameters considered in this procedure include positioning calculations. Subsequent technique in this paper proposes a real-time detection method of civilian stationary GPS receiver spoofing being implemented on a software-defined radio. As mentioned above, WT is an efficient tool for analyzing GPS signals (Azarbad & Mosavi, 2014; Mosavi & Azarbad, 2013). In fact, we performed an SWT-based denoising procedure in our anti-spoofing procedure on positioning residuals. By using SWT instead of standard WT, the coefficients created are more than sufficient to reconstruct the original signal. This causes additional choices for selecting the required coefficients and hence the algorithm performance can be improved by selecting better coefficients among all existing ones. Positioning differences are utilized as the inputs of SWT. Then, the receiver coordinates are achieved by the averaging function.

The proposed spoofing extraction and reduction algorithm consists of five main steps:

- **Step 1:** determining immediate interference.
- **Step 2**: Decomposing GPS coordinate residuals with SWT decomposition equation.
- **Step 3:** Thresholding operation to change the coefficients obtained from step 2.
- **Step 4:** Reconstructing the denoised SWT coefficients obtained from the previous stage.
- **Step 5:** Reducing the extracted position error from the primary position coordinates (Donoho & Johnstone, 1994).

To modify the coefficients in step 3, a rule of shrinkage should be chosen as stated in the pervious sections. Thresholding is performed by determining the method of coefficients reformation and the noise model (Azarbad & Mosavi, 2014). The SWT is an inherent redundant scheme, as each set of coefficients contains the same number of samples as the input and then for a decomposition of N levels, there is a redundancy of 2N. Since the SWT results in the coefficients redundancy, the reconstruction procedure is different from the same process used in the standard WT (Mosavi & Azarbad, 2014).

It is worth emphasizing that after the denoising procedure is finished in this phase, spoofing error is only the inaccuracy in the position estimations. In order to negate this position error, the position disturbance released from the third stage should be subtracted from the primary stationary GPS receiver location. The theoretical foundation of this algorithm for spoofing reduction operation in the GPS signal is based on the following discussion. If we assume the last authentic position before detecting spoofing signal is P_A, it contains noise and true position as:

$$P_A = P + N \tag{4}$$

Where P demonstrates the correct position and N is the noise. In this case, the position coordinates after acquiring spoofing signal can be written as follows:

$$P_C = P_A + S = P + N + S \tag{5}$$

Where P_C indicates the counterfeit location coordinates and S is spoofing differences. The difference of coordinates before and after spoofing detection in Easting, Northing and Upping (ENU) coordinates is applied to WT.

$$P_C - P_A = S + \Delta N \tag{6}$$

Coordinate residuals of the stationary GPS receiver are passed through SWT. Wavelet will extract spoofing error by providing the denoising process. We should subtract the extracted spoofing disturbance from the primary fake position solution to get the authentic location. Then, the receiver position is achieved by the averaging function (Worrall & Nebot, 2007). Fig. 2 describes the suggested algorithm in details. As a privilege, this algorithm makes no muddle if applied to an authentic signal. In other words, under the condition that the detector announces a false attack alarm and the algorithm is activated in normal mode, the final position will be genuine any way. Moreover, position accuracy may be modified due to the denoising procedure of WT. It is worth mentioning that the first authentic position is the last position just before spoofing detection and the next prestigious positions are obtained by applying WT.

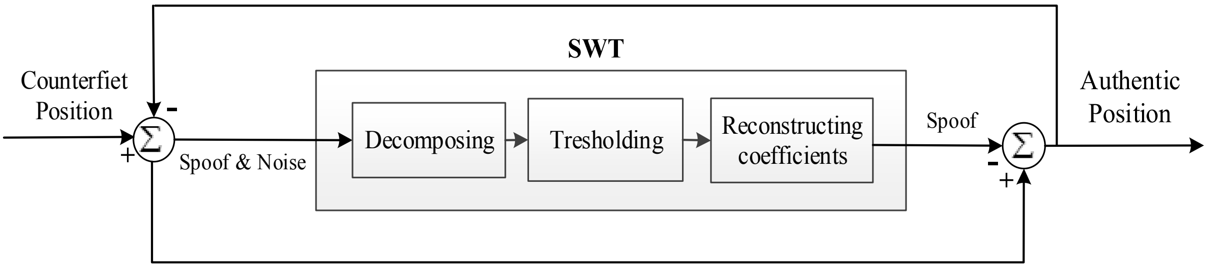

Figure 2. Proposed anti-spoofing algorithm

Simulation Results and Analysis

In order to investigate the performance of the suggested technique, we have implemented and tested our proposed plan with five different data sets separately to a stationary GPS receiver.

Counterfeit Data Generation

We combined a GPS software receiver with a transmitting RF front-end for practical implementation of an intermediate attacker. To construct the counterfeit data, a specific period of the input signal is delayed as a proper time and then combined with the authentic signals. This part provides a mathematical description of the data collection process (Mosavi & Azarbad, 2013). The processed signal in single-frequency civil GPS receivers takes the form of:

$$S_{L1_{CA}}(t) = A_C C_i(t) D_i(t) \sin(w_{L1}(t) + \phi_{L1}) \tag{7}$$

In this way, the constructed counterfeit signal can be written as:

$$\begin{aligned} C_{L1_{CA}}(t) = {} & A_C^A\, C_i^A(t) D_i^A(t) \sin(w_{L1}(t - \Delta t_A) + \phi_{L1}^A) \\ & + A_C^D C_i^D(t)\, D_i^D(t) \sin(w_{L1}(t - \Delta t_D) + \phi_{L1}{}^D) \end{aligned} \tag{8}$$

Where A and D represent the authentic and delayed signal, respectively. The Eq. (8) is in fact the spreading signal for deception. This signal demonstrated as the delayed one will be combined with the authentic signal. After providing and transmitting the faked signal, the signal coming to the victim receiver can be expressed as:

$$R_{L1_{CA}}(t) = S_{L1_{CA}}(t) + C_{L1_{CA}}(t) \tag{9}$$

In this procedure, two parameters are effective: delay time and delayed signal amplitude. In our experiment, the delay time is changed from 20 msec to 2 minutes in steps of 20 msec to generate different data sets. We know that the power of received GPS signal is low on the surface of the Earth (Mosavi & Azarbad, 2013). For negating the authentic signal at the stationary GPS receiver, the power of the constructed counterfeit signal can be increased (Lin et al., 2007) and adjusted higher than the authentic one in order to successfully mislead the target receiver and prevent simple detection (Ledvina et al., 2010) Also the amplitude of the delayed signal is selected as twice or triple the authentic one to be dominant in the target receiver. Therefore, Eq. (9) can be approximated as:

$$R_{L1_{CA}}(t) \approx C_{L1_{CA}} \tag{10}$$

Details of the produced spoofing data sets are reported in Table 1, that can spoof the victim single frequency GPS receiver from 646 meters to 2083 meters.

Test Results

The results of the simulations were analyzed in personal computer using Matlab software (Borre et al., 2007). The generated spoofing error and the percentage of spoofing reduction is reported in Table 2.

Each row of the table relates to results of the proposed anti-spoofing algorithm by specified mother wavelets on different spoofing dataset. The mitigation average column indicates mean of reduction percentages for every WT. The difference between the highest and lowest spoofing reduction percentages of different spoofing data for each WT

is reported as tolerance in the right column of the table.
So, as can be seen in Table 2, we can mitigate spoofing more than 93% within a tolerant less than 6% and an average of 93.57%. Spoofing errors are depicted in Figs. 3 to 7 before and after applying the suggested algorithm by using the dmey WT in level 3.

A great improvement of the proposed method is obvious in all of the figures for its quick detection of spoofing. Because of the dissimilarity between this method and the existing ones, making an accurate comparison with the prior works is difficult. In Table 3, the proposed technique is compared with two samples from variant views. The discussed results show that the proposed method brings an outstanding performance in spoofing reduction.

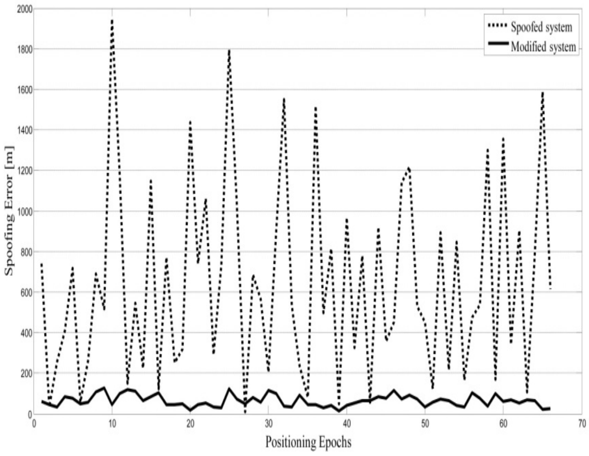

Figure 3. Positioning error in the first data set before and after applying the anti-spoofing algorithm

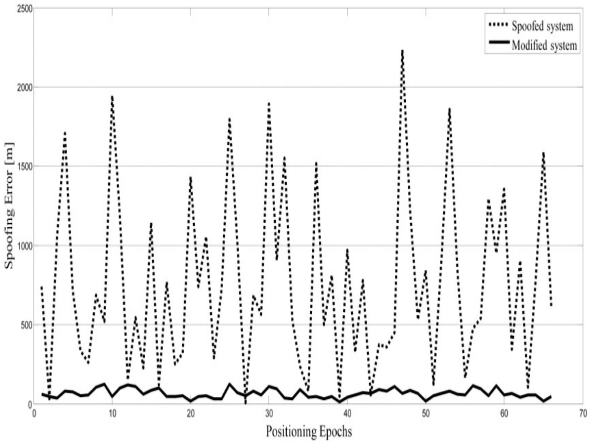

Figure 4. Positioning error in the second data set before and after applying the anti-spoofing algorithm

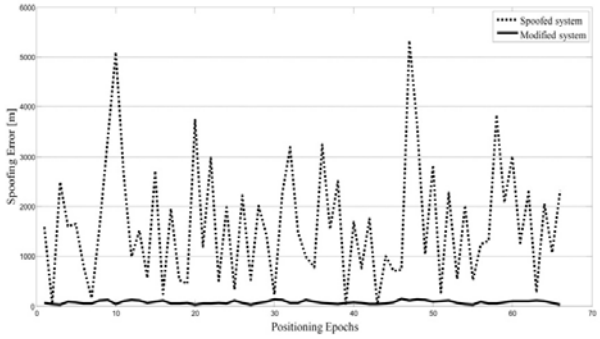

Figure 5. Positioning error in the third data set before and after applying the anti-spoofing algorithm

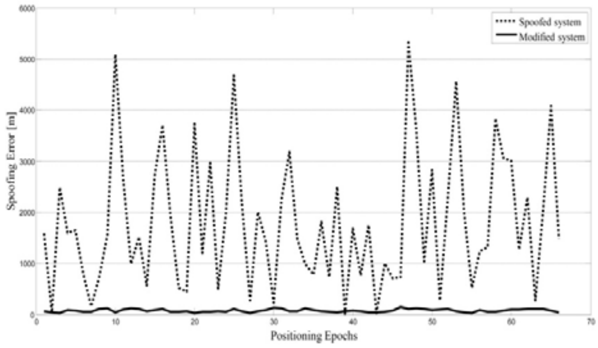

Figure 6. Positioning error in the fourth data set before and after applying the anti-spoofing algorithm

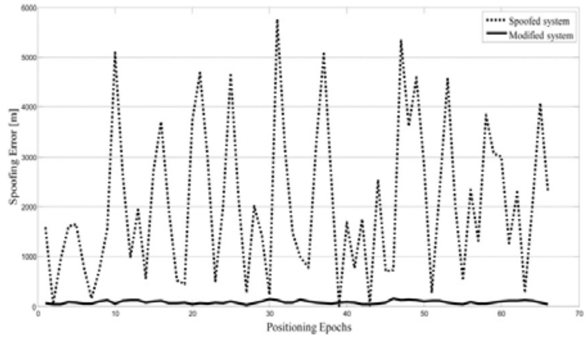

Figure 7. Positioning error in the fifth data set before and after applying the anti-spoofing algorithm

Table 1. Details of spoofing data sets

Data Sets	ΔE [m]	ΔN [m]	ΔU [m]	ΔRMS [m]
First	17	149	628	646
Second	19	171	739	759
Third	394	435	1395	1513
Fourth	466	518	1660	1800
Fifth	540	593	1922	2083

Table 2. Details of anti-spoofing algorithm performance

WT	Level	Spoofing value in meters					Mitigation average (%)	Tolerance (%)
		646	**759**	**1651**	**1800**	**2083**		
		Mitigation percent						
dmey	3	90	91	95	96	96	93.6	6
sym-4	3	92	95	92	94	95	93.6	3
db-10	2	90	94	94	95	96	93.8	6
coif-3	5	91	94	92	94	94	93	3
bior-2.2	3	90	93	93	95	95	93.2	5
rbio-1.3	2	91	96	93	95	96	94.2	5

Table 3 Comparison with prior works

Spoofing reduction method	Implementation	Primary spoofing error [m]	Mitigation	Change in receiver	algorithm implementation position	Kind of spoofing
This work (5th data set)	Simulation	2083	95.3% [a]	No	Navigation	Delay and mixing procedure
(Jahromi et al., 2012b)	Simulation	1800	85% [b]	Yes	Tracking & navigation	Code phase modulation
(Nielsen et al., 2012)	Statistical analysis	500-1500	74%	No	Acquisition & tracking	Code phase modulation

a. Extracted by averaging.
b. Extracted from position curve.

Conclusion

In this paper, attacks and interference rejection techniques have been briefly reviewed. WT as a strong tool has been introduced and a new interference mitigation technique based on wavelet denoising has been proposed. We designed an algorithm by SWT to compensate the spoofing effect on GPS signal. It is suggested that a real-time detection method of civilian stationary GPS receiver spoofing be implemented. Positioning differences have been utilized as the inputs of the SWT. Then, the receiver coordinates are obtained by the averaging function. The suggested technique for stationary application can obviously attenuate the effectiveness of spoofer. Finally, the civil stationary GPS receivers could be immediately modified to exploit the proposed authentication strategy.

References

1. Azarbad, M.R. and Mosavi, M.R., “A New Method to Mitigate Multipath Error in Single-Frequency GPS Receiver with Wavelet Transform,” *Journal of GPS Solutions*, Vol. 18, No. 2, 2014, pp. 189-198.
2. Borre, K., Akos, D.M., Bertelsen, N., Rinder, P. and Jensen, S.H., *A Software-Defined GPS and Galileo Receiver: A Single-Frequency Approach*, Boston: Birkhäuser.
3. Chang, C.J., Time Frequency Analysis and Wavelet Transform Tutorial, Time-Frequency Analysis for Biomedical Engineering, Institute of Communication Engineering, National Taiwan University, 2014, pp. 1-22.
4. Collin, F. and Warnant, R., “Applications of the Wavelet Transform for GPS Cycle Slip Correction and Comparison with Kalman Filter,” *Manuscripta Geodaetica*, Vol. 20, 1995, pp. 161-172.
5. Daneshmand, S., A.J., Broumandan, A. and Lachapelle, G., “A Low Complexity GNSS Spoofing Mitigation Technique using a Double Antenna Array,” *GPS World Magazine,* Vol. 22, No. 12, pp. 44-46.
6. Daneshmand, S., Jahromi, A.J., Broumandan, A. and Lachapelle, G., “GNSS Spoofing Mitigation in Multipath Environments using Space-Time Processing,” *European Navigation Conference*, 2013, pp. 1-12.
7. Donoho, D.L. and Johnstone, I.M., “Threshold Selection for Wavelet Shrinkage of Noisy Data, IEEE Conference on Engineering in Medicine and Biology Society,” *Engineering Advances: New Opportunities for Biomedical Engineers*, Vol. 1, 1994, pp. 24-25.
8. Fu, W.X. and Rizos, C., “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, 1997, pp. 1385-1388.
9. Humphreys, T.E., Bhatti, J., and Ledvina, B., “The GPS Assimilator: a Method for Upgrading Existing GPS User Equipment to Improve Accuracy,” *Robustness and Resistance to Spoofing, The 23rd International Technical Meeting of the Satellite Division of the Institute of Navigation*, 2010, pp. 1-11.
10. Humphreys, T.E., Ledvina, B.M., Psiaki, M.L., O'Hanlon, B.W., and Kintner, P.M., Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer, *The 21st International Technical Meeting of the Satellite Division of the Institute of Navigation*, 2008, pp. 2314-2325.
11. Jahromi, A.J., Broumandan, A., Nielsen, J., and Lachapelle, G., “GPS Vulnerability to Spoofing Threats

and a Review of Antispoofing Techniques," *Journal of Navigation and Observation*, 2012a, pp. 1-16.

12. Jahromi, A.J., Lin, T., Broumandan, A., Nielsen, J. and Lachapelle, G., Detection and Mitigation of Spoofing Attacks on a Vector-Based Tracking GPS Receiver, *International Technical Meeting of the Institute of Navigation*, 2012b, pp. 3-8.
13. Jin, M.H., Han, Y.H., Choi, H.H., Park, C., Heo, M.B., and Lee, S.J., "GPS Spoofing Signal Detection and Compensation Method in DGPS Reference Station," *The 11th International Conference on Control, Automation and Systems*, 2011, pp. 1616-1619.
14. Ledvina, B.M., Bencze, W.J., Galusha, B., and Miller, I., "An In-Line Anti-Spoofing Device for Legacy Civil GPS Receivers," *The 23rd International Technical Meeting of the Institute of Navigation*, 2010, pp. 689-712.
15. Lin, Z., Haibin, C. and Naitong, Z., "Anti-Spoofing Extended Kalman Filter for Satellite Navigatin Receiver," *IEEE Conference on Wireless Communications, Networking and Mobile Computing*, 2007, pp. 996-999.
16. Mosavi, M.R., "Comparing DGPS Corrections Prediction using Neural Network, Fuzzy Neural Network and Kalman Filter," *Journal of GPS Solutions*, Vol. 10, No. 2, 2006, pp. 97-107.
17. Mosavi, M.R., and Azarbad, M.R.,. Multipath Error Mitigation based on Wavelet Transform in L1 GPS Receivers for Kinematic Applications. International *Journal of Electronics and Communications*, Vol. 67, No. 10, 2013, pp. 875-884.
18. McDowell, C.E., GPS Spoofer and Repeater Mitigation System using Digital Spatial Nulling, U.S. Patent 7250903 B1.
19. Merry, R.J.E., Wavelet Theory and Applications, Eindhoven University of Technology Department of Mechanical Engineering Control Systems Technology Group, A Literature Study.
20. Ogaja, C., Rizos, C., Wang, J. and Brownjohn, J., "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*, 2001, pp. 284-293.
21. Nielsen, J., Broumandan, A. and Lachapelle, G., Spoofing Detection and Mitigation with a Moving Handheld Receiver, *GPS World Magazine*, Vol. 21, No. 9, 2010, pp. 27-33.
22. Nielsen, J., Dehghanian, V. and Lachapelle, G., "Effectiveness of GNSS Spoofing Countermeasure based on Receiver CNR Measurements," *International Journal of Navigation and Observation*, 2012, pp. 1-9.
23. Papadimitratos, P., and Jovanovic, A.,. "GNSS-Based Positioning: Attacks and Countermeasures," *IEEE Military Communications Conference*, 2008, pp. 1-8.
24. Satirapod, C., Improving the GPS Data Processing Algorithm for Precise Static Relative Positioning', [Ph.D. Thesis], School of Surveying & Spatial Information Systems, The University of New South Wales, Sydney, Australia.
25. Satirapod, C., Wang, J., and Rizos, C.,. Comparing Different GPS Data Processing Techniques for Modelling Residual Systematic Errors, Journal of Survey Engineering, Vol. 129, No. 4, 2003, pp. 129-135.
26. Souza, M., Monico, J.F.G., Pagamisse, A. and Polezel, W.G.C., "An Effective Wavelet Method to Detect and Mitigate Low-Frequency Multipath Effects," *International Association of Geodesy Symposia*, Vol. 132, 2008, pp. 179-184.
27. Wesson, K.D., Shepard, D.P., Bhatti, J.A. and Humphreys, T.E., "An Evaluation of the Vestigial Signal Defense for Civil GPS Anti-Spoofing," *24th International Technical Meeting of the Satellite Division of the Institute of Navigation*, 2011, pp. 1-11.
28. Worrall, S. and Nebot, E., "Automated Process for Generating Digitized Map Through GPS Data Compression," *Australasian Conference on Robotics & Automation*, 2007, pp. 1-6.