ICIC Express Letters
Volume **11**, Number **3**, March **2017**

ICIC International ©2017 ISSN 1881-803X
pp. 681–688

A NOVEL SPOOFING DETECTION AND MITIGATION ALGORITHM BASED ON GNSS/INS COMBINED VECTOR TRACKING LOOPS

Fei Xie[1,4], Jing Zhao[2,4,*], Weixing Qian[1] and Yufei Xu[3]

[1]School of Electrical and Automation Engineering
Nanjing Normal University
[4]Jiangsu Key Laboratory of 3D Printing Equipment and Manufacturing
No. 78, Bancang Street, Nanjing 210042, P. R. China

[2]School of Automation
Nanjing University of Posts and Telecommunications
No. 9, Wenyuan Road, Yadong New District, Nanjing 210023, P. R. China
*Corresponding author: zhaojing@njupt.edu.cn

[3]Shanghai Institute of Satellite Engineering
No. 251, Huaning Road, Minhang District, Shanghai 200240, P. R. China

Received August 2016; accepted November 2016

Abstract. *There is an increasing concern that the civil global navigation satellite system (GNSS) signals are highly vulnerable to malicious jamming and spoofing attacks that deceive a victim receiver into locating counterfeit position. To solve this problem, a novel spoofing detection and mitigation algorithm based on GNSS/INS combined vector tracking loops is proposed. Firstly, the aggregation of two detection approaches including signal power analysis and spatial correlation method is used to detect the presence of counterfeit spoofing signals. Secondly, a novel spoofing mitigation algorithm based on GNSS/INS combined vector tracking loops is developed, which takes advantage of the intrinsic relationships between authentic signal's code phase and carrier frequency biases and INS navigation solution. Finally, simulation tests are carried out with a signal simulator and a software receiver. The test results indicate that the proposed spoofing detection and mitigation algorithm has an anti-spoofing and jamming tolerant capability under civilian spoofing interference environments.*

Keywords: GNSS navigation, Anti-spoofing, Software receiver, Vector tracking

1. Introduction.

There is an increasing attention to secure and reliable GNSS applications such as transportations, air, marine, telecommunication systems, and mobile phone location. Especially, most mobile phones as well as vehicles are equipped with navigation and positioning systems using GPS nowadays. GNSS spoofing threat has become a hot topic since the Iranians had captured a highly classified Central Intelligence Agency drone, a stealth Lockheed Martin RQ-170 Sentinel, purportedly by spoofing its GPS equipment. Fast forward to today, GPS and other GNSS are also susceptible to meaconing. GPS signals are vulnerable to in-band electromagnetic interferences because of extremely weak signals broadcasted from the satellites. GPS signals strength may be as low as$-$160dBW watts when the signals reach the earth surface, which lead to a spectrum spread out below the noise floor in the receivers. Under this condition, interference with this low signal strength can easily defeat signal recovery or overload the receiver circuitry, resulting in loss of the positioning and timing service [1].

Actually, effective techniques indeed exist to defend receivers against GNSS spoofing attacks. On the one hand, cryptographic techniques are the most effective way against GNSS spoofing. Military GPS receivers have long been protected against spoofing attack by selective availability anti-spoofing module (SAASM) [2]. Anti-spoofing (AS) is a protection against fake transmissions by encrypting the P-code to form the Y-code. This ensures that the GPS signals cannot be disturbed by a GPS-like transmitter on the earth. Moreover, the anti-spoofing procedure converts the P-code to the Y-code which is only usable when a secret conversion algorithm is available to the receiver [1]. However, only selected users have access to the conversion algorithm. The effect of AS is that civilian users have only access to the C/A code and therefore are easily attacked and spoofed. On the other hand, several civilian spoofing countermeasure techniques have been proposed by many researchers [3-11]. Nielsen et al. make use of the pairwise correlation feature of signals from different PRNs for a moving receiver to detect the spoofing signals that are transmitted by a same spoofer antenna [3]. Actually, a spoofer generates multiple fake GNSS signals and transmits them using a single antenna while the authentic signals are transmitted from different satellites with different directions. In this practical case, spoofing signals corresponding to different PRNs are spatially correlated because they all have the same propagation path. McDowell takes advantage of this feature to discriminate spoofing signals based on their phase variations using multiple GNSS antennas [4]. Montgomery et al. propose a spoofing detection approach which observes the phase difference between two fixed antennas for around one hour [5]. However, antenna array processing produces unpredictable biases in receiver measurements, and additional hardware complexity or computational burden to the receiver. Besides, in open sky conditions, only satellite movement and ionosphere variations can cause gradual smooth changes in the received signal power [6]. Hence, some spoofing mitigation techniques rely on abnormal signal power monitoring to detect the spoofing signals. Nielsen et al. successfully detect the presence of high-power spoofing signals through their abnormally high C/N0 values [7]. Although the above mentioned approaches can effectively detect the spoofing attack in specific situations, there are still many challenges in terms of anti-spoofing receiver research and development, for example, how to classify the spoofing signals from the authentic ones based on the receiver motion feature by incorporating a low-cost IMU in the receiver. Compared with published literature in the field of anti-spoofing research, this paper makes two contributions: (i) the intrinsic relationships between authentic signal's code phase and carrier frequency biases and INS navigation solution have been analyzed; (ii) a novel spoofing detection and mitigation algorithm based on GNSS/INS combined vector tracking loops has been proposed to detect spoofing signals and enables the receiver to adapt with signal jamming and spoofing environments.

This paper is organized as follows. In Section 2, the spoofing signal model and our solution to the spoofing threat are analyzed to reveal the inherent mechanism of spoofing attacks. Section 3 mainly proposes a novel spoofing signal detection and mitigation algorithm based on GNSS/INS combined vector tracking loops. Additionally, experimental results are given in Section 4. Finally, conclusion and future work are drawn in Section 5.

2. The Spoofing Signal Model and Threat Solution.

Spoofing is the transmission of interference signals whose structure matches authentic GNSS signal that aims to control the tracking loops of a victim receiver and thereby mislead the receiver's timing or navigation solution [12]. Hence, the spoofing transmitter tries to mimic the authentic signals' structure and modulate the same signal parameters in the spoofing signal. Take GPS L1 civilian signal for example, it is assumed that the receiver is subjected to a spoofing attack, and the received signal including the authentic signal and spoofing signal can be modeled as:

$$\begin{aligned} S_{as}(t) = & \sum_{i=1}^{n} A_{a,i} d_{a,i}(t-\tau_{a,i}) c_{a,i}(t-\tau_{a,i}) e^{j2\pi t f_{d,i}} \\ & + \sum_{i=1}^{m} A_{s,i} d_{s,i}(t-\tau_{s,i}) c_{s,i}(t-\tau_{s,i}) e^{j2\pi t f_{sd,i}} + \varsigma(t) \end{aligned} \quad (1)$$

where the subscripts a and s represent authentic and spoofing signals respectively. i is the channel number, whose total number is n and m respectively. A is the incoming signal amplitude; d is the navigation data; $c(t)$ is the pseudo-random code sequence; τ is the replica code's phase bias in units of chips; f_d is the replica carrier's Doppler frequency in units of Hz; $\varsigma(t)$ is the additional white Gaussian noise with variance σ^2.

When an anti-spoofing GNSS receiver is turned on, the following operations must be done in sequence before the receiver can demodulate the navigation data and use it to provide a navigation solution.

1) Search for the received signal and determine the approximate code delay and carrier frequency of each visible satellite;
2) Detect whether or not a possible spoofing attack is performed to receiver using the aggregation of signal power monitoring and spatial correlation method;
3) If a spoofing attack is detected, an authentic signal reconstruction is implemented to mitigate the spoofing components from the received IF signals;
4) Track the code delay and carrier frequency using the proposed GNSS/INS combined vector tracking method as the relative position of satellites and receiver changes and keep the authentic signals in lock.

According to analysis of Akos's research group [13], when a spoofing signal is transmitted by a malicious source, the received signal's power can highly vary once the propagation distance between the spoofer and the disturbed receiver has changed. Therefore, the sudden variation of the received signal power level can be used to reveal the presence of a potential spoofing attack firstly.

Then, it is assumed that the spoofing signal is well disguised, to say the least. The received signal will be detected next using the proposed spatial correlation method. Specifically, the autocorrelation and cross correlation properties of the pseudo-random codes are exploited to determine the phase of the spread spectrum code in signal acquisition processing section of GNSS receiver. When one spoofing signal is generated and enters into the target receiver with the authentic signal, two acquisition results may appear:

(1) The real visible satellite is detected, but two correlation peaks are searched. This reveals that the spoofing signal mimics the signal structure of real visible satellites, but using a different code delay. This spoofing signal can be classified by spatial correlation method;

(2) The disguised visible satellites are not detected, since only one correlation peak is found for each satellite. This reveals the spoofer simulated some unreal signals in the open sky, and their structure may be very similar to the authentic signals. Meanwhile, they also can be demodulated by the receiver and used to provide navigation solution. In order to deal with this spoofing signal, a GNSS/INS combined vector tracking method is proposed.

3. **The Spoofing Signal Detection and Mitigation Algorithm.**

This section presents a novel spoofing signal detection and mitigation method based on GNSS/INS combined vector tracking loops, which is shown in Figure 1. In a traditional GNSS receiver, each tracking channel exploits the scalar tracking architecture to estimate the pseudorange and pseudorange-rate measurements independently for the visible satellites.

Compared to using conventional scalar tracking loop to track each satellite independently, the vector tracking loop takes advantage of the correlation between each satellite and receiver movements and use a single Kalman filter to accomplish the signal tracking and position, velocity, and time estimation simultaneously. As Figure 1 shows, the state vector of the pre-filter is defined as:

$$x_{p,i} = \begin{pmatrix} A_i & \tau_i & \delta\phi_i & \delta f_{d,i} & \delta\dot{f}_{d,i} \end{pmatrix} \tag{2}$$

where A and τ have the same meaning with Equation (1). $\delta\phi$ is the replica carrier phase bias. $\delta f_{d,i}$ is the replica carrier's Doppler frequency bias for the i-th satellite. $\delta\dot{f}_d$ is the replica carrier's Doppler frequency rate bias. The measurements are derived from the six correlators' outputs $I_{E,i}$ $Q_{E,i}$ $I_{P,i}$ $Q_{P,i}$ $I_{L,i}$ $Q_{L,i}$ available for each channel. They are used to update the vector tracking pre-filters and can be written as follows:

$$z_{p,i} = \begin{pmatrix} I_{E,i} & Q_{E,i} & I_{P,i} & Q_{P,i} & I_{L,i} & Q_{L,i} \end{pmatrix} \tag{3}$$

The measurement equation can be shown as:

$$z_{p,k} = h_k x_k + v_k \tag{4}$$

where $z_{p,k}$ is the measurement vector. h_k is the nonlinear measurement matrix at k time. v is measurement noise vector, which can be seen as zero-mean white Gaussian noise.

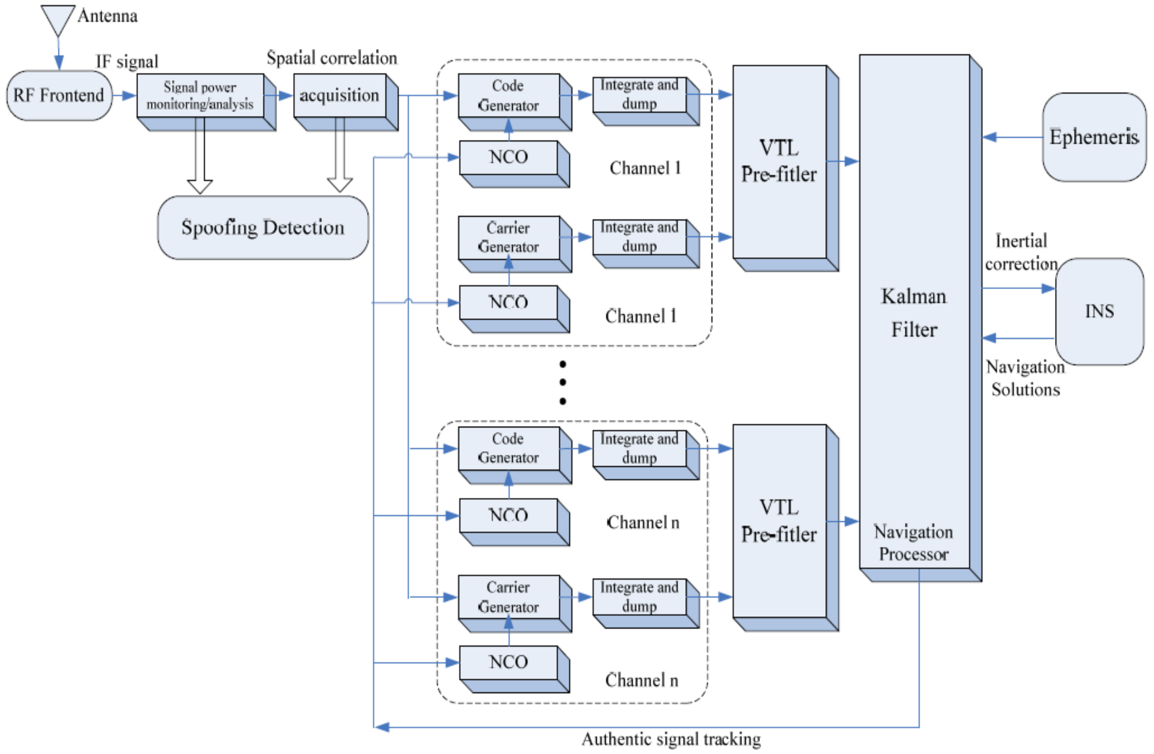

Figure 1. GNSS/INS combined anti-spoofing vector tracking architecture

As the goal is to combine the authentic signals' tracking and INS navigation states together, deep fusion of the combined vector tracking loop and INS states is accomplished by an integrated Kalman filter. The states of the integrated filter are shown in Equation (5) for combined GNSS/INS systems.

$$\begin{aligned} X_I = (&\delta x_I \quad \delta y_I \quad \delta z_I \quad \delta\dot{x}_I \quad \delta\dot{y}_I \quad \delta\dot{z}_I \quad \varphi_e \quad \varphi_n \quad \varphi_u \quad \varepsilon_{bx} \\ &\varepsilon_{by} \quad \varepsilon_{bz} \quad \varepsilon_{rx} \quad \varepsilon_{ry} \quad \varepsilon_{rz} \quad \nabla_x \quad \nabla_y \quad \nabla_z \quad \delta t_u \quad \delta f_u) \end{aligned} \tag{5}$$

where the first eighteen states indicate three position errors, three velocity errors, three attitude errors, gyroscope drift bias and acceleration bias respectively in the INS, in which the position and velocity states are expressed in the earth frame. The last two states δt_u and δf_u are the receiver clock bias and clock drift respectively. Besides, in order to analyze the principle of the proposed anti-spoofing method based on GNSS/INS combined vector tracking loops, the intrinsic relationships between authentic signal's code phase and carrier frequency biases and INS navigation solution have been provided here:

$$\begin{aligned} \lambda_{code}\tau_{a,i} &= \rho_{Ii} - \rho_{Gi} \\ &= r_i + e_{i1}\delta x_I + e_{i2}\delta y_I + e_{i3}\delta z_I - (r_i + c \cdot \delta t_u - c \cdot \delta t_{SVi} + c \cdot \delta t_{atmos} + \varepsilon_{\rho_i}) \end{aligned}$$

$$
\begin{aligned}
&= e_{i1}\delta x_I + e_{i2}\delta y_I + e_{i3}\delta z_I - c\cdot(\delta t_u - \delta t_{SVi} + \delta t_{atmos}) - \varepsilon_{\rho_i} \qquad (6)\\
\lambda_{RF}\delta f_{a,di} &= \dot{\rho}_{Ii} - \dot{\rho}_{Gi}\\
&= \dot{\rho}_{Ii} - (\dot{r}_i - \delta f_u + \delta f_{SVi} + \varepsilon_{\dot{\rho}_i})\\
&= e_{i1}\delta\dot{x}_I + e_{i2}\delta\dot{y}_I + e_{i3}\delta\dot{z}_I + \delta f_u - \delta f_{SVi} - \varepsilon_{\dot{\rho}_i} \qquad (7)
\end{aligned}
$$

where the terms λ_{code} and λ_{RF} denote the wavelength of the code and radio frequency signals, respectively. ρ_{Ii}, $\dot{\rho}_{Ii}$ and ρ_{Gi}, $\dot{\rho}_{Gi}$ denote the pseudorange and pseudorange rate calculated by INS and GNSS receiver, respectively. r_i and $\dot{r}_i$ denote the actual range and range rate between the i-th satellite and the receiver, respectively. δt_{SV} and δf_{SV} denote the clock error and its change rate of satellite. e_{i1}, e_{i2}, e_{i3} are the components of unit vector in the line-of-sight direction from receiver to the i-th satellite. δt_{atmos} is the atmospheric propagation delay. c is the speed of light. ε_{ρ_i} and $\varepsilon_{\dot{\rho}_i}$ denote the noise terms.

The outputs of the combined vector tracking pre-filters are actually the measurements needed by the integrated filter. The measurement of the integrated filter can be written as:

$$Z_I = (\lambda_{code}\tau_1, \cdots, \lambda_{code}\tau_n, \lambda_{RF}\delta f_{d,1}, \cdots, \lambda_{RF}\delta f_{d,n})^T \qquad (8)$$

In order to track the authentic signals using the actual receiver movement states, the integrated Kalman filter sends control commands to each channel's tracking NCO, which drive the tracking loop to generate the replica code and carrier signals and demodulate the authentic signals. The feedback commands can be written as follows:

$$f_{code_i,k+1} = f_{code_i,k} + \Delta\hat{f}_{\tau_i,k+1} + \frac{\lambda_{RF}}{\lambda_{code}}\cdot\Delta\hat{f}_{carr_i,k+1} \qquad (9)$$

$$\Delta\hat{f}_{\tau_i,k+1} = \frac{\tau_i}{\Delta t} = \frac{1}{\Delta t}\frac{1}{\lambda_{code}}(\rho_{Gi,k+1} - \hat{\rho}_{i,k+1}) \qquad (10)$$

$$f_{carr_i,k+1} = f_{carr_i,k} + \Delta\hat{f}_{d_i,k+1} + \Delta t\cdot\Delta\hat{\dot{f}}_{d_i,k+1} \qquad (11)$$

where $\Delta\hat{f}_{\tau_i,k+1}$ is the pseudorange change corresponding to the code phase correction estimated by the predicted position at the time of $k+1$. The terms $\Delta\hat{f}_{d_i}$ and $\Delta\hat{f}_{carr_i}$ denote the changes in the Doppler frequency and carrier frequency, respectively. And $\Delta\hat{\dot{f}}_{d_i}$ is the change rate of Doppler frequency. $\hat{\rho}_i$ is the pseudorange estimate between the i-th satellite and the receiver, which can be calculated from predicted INS navigation position. The receiver will update the loop NCO at an interval of Δt in the vector tracking process. The feedback commands by the integrated filter enable the receiver to obtain the ability to track the authentic signals after spoofing signal is temporarily sampled.

4. **Test Results and Analysis.** Testing a spoofing interference in a real case is challenging since outdoor spoofing signal transmission in the GNSS frequency bands is not allowed. In order to test and verify performance of the proposed GNSS/INS combined spoofing detection algorithm, simulation tests are carried out. Simulation platform consists of a GPS L1 signal simulator and a base band signal development board including the front end. The output of this board is a pair of streams IF samples, which are subsequently passed to the software receiver for vector tracking debugging and algorithm verification.

In order to demonstrate the performance of the proposed GNSS/INS combined spoofing discrimination algorithm in a jamming and spoofing environment, three tests involving signal power monitoring, spatial correlation and GNSS/INS combined spoofing detection methods have been implemented. Firstly, the target receiver is fed with the sum of the authentic and highly power spoofing signal. The power gain of authentic signals can reach 45 to 47 dB, while that of the spoofing signals in each channel can reach 55 to 60 dB, which can be seen in Figure 2. After multiple experimental results analysis, if the power of spoofing signal is too low, the target receiver never tracks counterfeit signals. If too

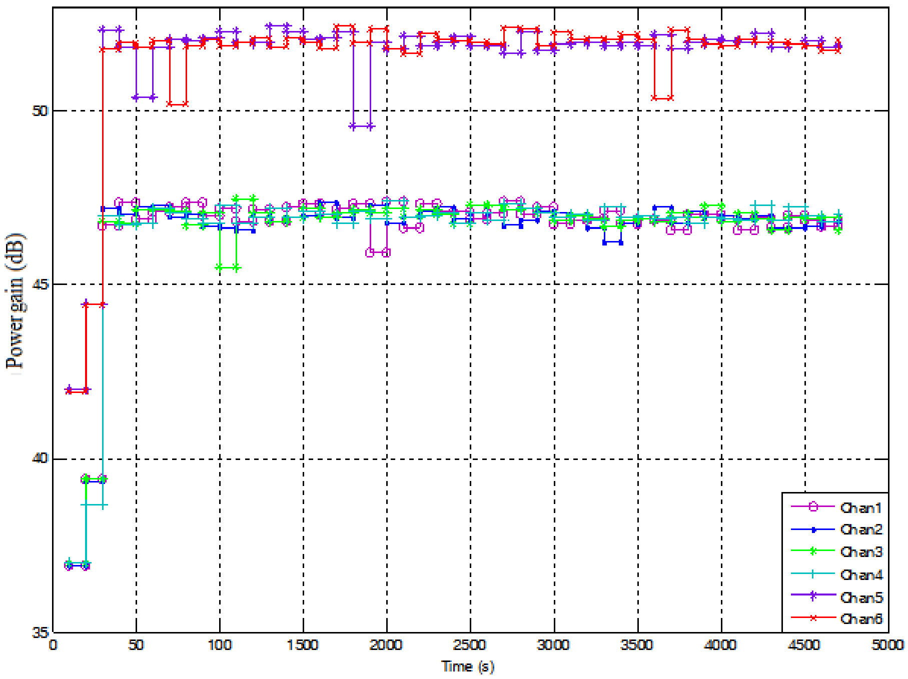

Figure 2. Comparison of power gain between spoofing and authentic signals

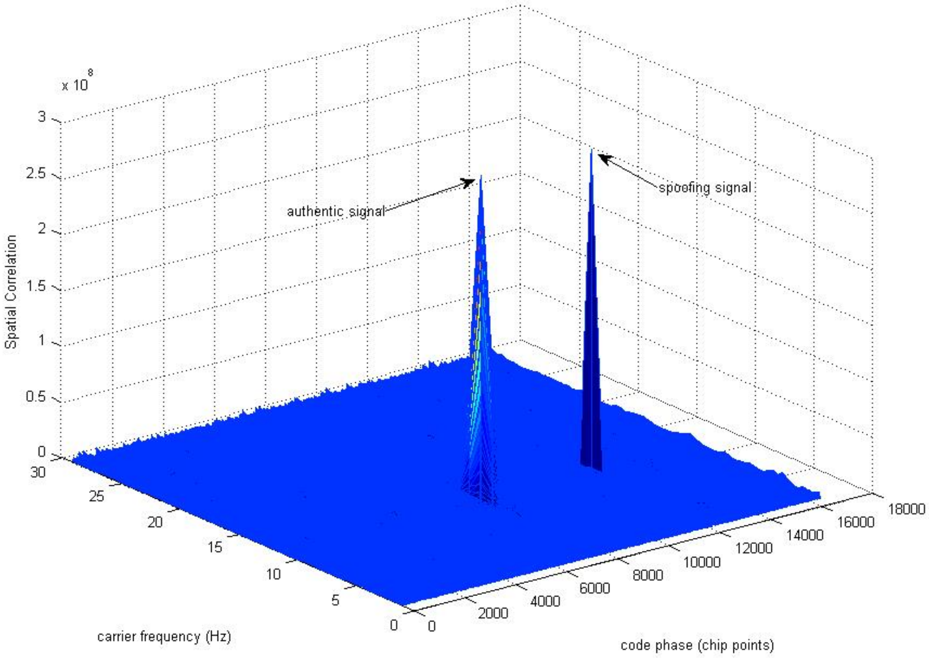

Figure 3. Spatial correlation results of spoofing and authentic signals

high, the spoofing signal is easily identified and classified. Therefore, degradation of the spoofing signal power by 10 dB is done afterwards, and then the authentic and spoofing signals both can be captured. In this case, it can be seen from Figure 3 that two distinctive peaks are visible using the spatial correlation method in the acquisition process, where the stronger peak is the spoofing signal, and the weaker peak is the authentic signal. Once the spoofing signal is detected, the spoofing attack alarm is set and its measurement is isolated.

Finally, if the mimic spoofing signal is not detected in the stage of acquisition, then the GNSS/INS combined anti-spoofing vector tracking algorithm can be used to continue classifying authentic and spoofing signals. Figure 4 shows the tracking results which the spoofing signal was unable to be demodulated by GNSS/INS combined vector loops. On the contrary, the authentic signal was demodulated and locked successfully. So the receiver can recognize the spoofing attack independently and adapt with signal jamming and spoofing environments.

Figure 5 shows the detection results of the authentic and spoofing signals using spatial correlation method and GNSS/INS combined spoofing discrimination algorithm. As shown in Figure 5, the software receiver determinates five authentic signals and four

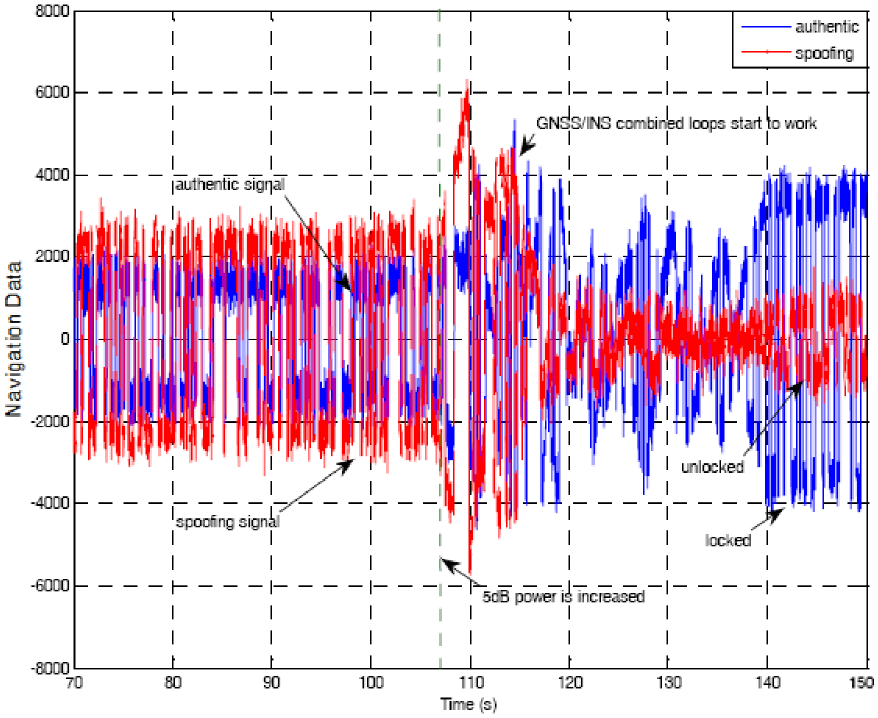

FIGURE 4. Tracking results using the proposed GNSS/INS combined vector loops

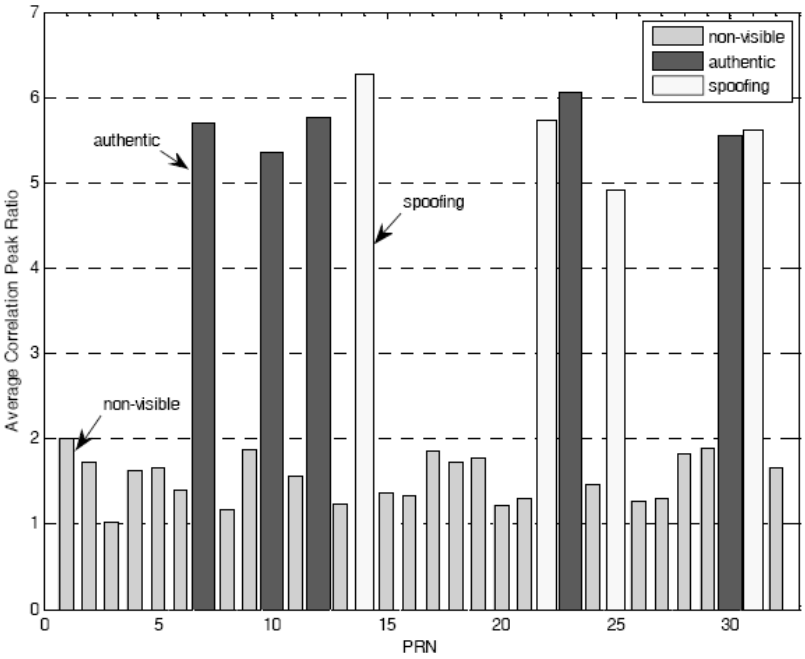

FIGURE 5. Spoofing and authentic signals classified results by the proposed algorithm

spoofing signals, namely PRNs 14, 22, 25 and 31. Importantly, these spoofing signals will subsequently be removed from the received if samples or their measurement in corresponding channel will be isolated when making a navigation calculation.

5. **Conclusion and Future Work.** This paper has presented a novel spoofing detection and mitigation algorithm based on GNSS/INS combined vector tracking loops. As the experimental results shown, the proposed anti-spoofing algorithm can effectively detect the presence of a spoofing attack in highly matched power level. As future work, the anti-spoofing technique based on combined multi-frequency receivers and INS should be further studied and developed to fit more complex jamming and spoofing environments.

Acknowledgment. This work is partially supported by the National Natural Science Foundation of China (Grant Nos. 61601228, 61403210, 61603191), and the Natural Science Foundation of Jiangsu Higher Education Institution (15KJB510016), Natural Science Foundation of Jiangsu (BK20161021, BK20141453) and sponsored by NUPTSF (NY214173), and the Open Program of Jiangsu Key Laboratory of 3D Printing Equipment and Manufacturing, Item Number 3DL201607. The authors gratefully acknowledge the helpful comments and suggestions of the reviewers for valuable remarks.

REFERENCES

[1] D. Shepard and T. E. Humphreys, Characterization of receiver response to a spoofing attack, *Proc. of the 24th International Technical Meeting of the Satellite Division of the Institute of Navigation*, Portland, Ore, pp.2608-2618, 2011.

[2] M. L. Psiaki, S. P. Powell and B. W. O'Hanlon, Correlating carrier phase with rapid antenna motion, *GPS World*, vol.20, no.1, pp.28-35, 2013.

[3] J. Nielsen, A. Broumandan and G. Lachapelle, GNSS spoofing detection for single antenna handled receivers, *Navigation*, vol.58, no.4, pp.335-344, 2011.

[4] C. E. McDowell, *GPS Spoofer and Repeater Mitigation System Using Digital Spatial Nulling*, US Patent 7250903 B1, pp.1-7, 2007.

[5] P. Y. Montgomery, T. E Humphreys and B. M. Ledvina, Receiver-autonomous spoofing detection: Experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer, *Proc. of the 22nd International Technical Meeting of the Satellite Division of the Institute of Navigation*, Anaheim, CA, pp.124-130, 2009.

[6] A. Jafarnia, A. Broumandan, J. Nielsen and G. Lachapelle, GPS vulnerability to spoofing threats and a review of anti-spoofing techniques, *International Journal of Navigation and Observation*, vol.2, no.7, pp.20-26, 2012.

[7] J. Nielsen, V. Dehghanian and G. Lachapelle, Effectiveness of GNSS spoofing countermeasure based on receiver CNR measurements, *International Journal of Navigation and Observation*, vol.5, no.3, pp.31-40, 2012.

[8] M. L. Psiaki, B. W. O'Hanlon, J. A. Bhatti and D. P. Shepard, GPS spoofing detection via dual-receiver correlation of military signals, *IEEE Trans. Aerospace and Electronic Systems*, vol.49, no.4, pp.2250-2267, 2013.

[9] A. Broumandan, A. Jafarnia, V. Dehghanian et al., GNSS spoofing detection in handled receivers based on signal spatial correlation, *Proc. of IEEE/ION Position Location and Navigation Symposium*, Myrtle Beach, SC, pp.479-487, 2012.

[10] A. J. Jahromi, A. Broumandan, J. Nielsen and G. Lachapelle, GPS spoofer countermeasure effectiveness based on signal strength, noise power, and C/N0 measurements, *International Journal of Satellite Communications and Networking*, vol.30, no.4, pp.181-191, 2012.

[11] A. Jovanovic, C. Botteron and P. A. Farine, Multi-test detection and protection algorithm against spoofing attacks on GNSS receivers, *Proc. of IEEE/ION Position Location and Navigation Symposium*, Monterey, CA, pp.1258-1271, 2014.

[12] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki et al, Assessing the spoofing threat: Development of a portable GPS civilian spoofer, *Proc. of ION GNSS*, Savannah, GA, pp.2314-2325, 2008.

[13] D. M. Akos, Who's afraid of the spoofer? GPS/GNSS spoofing detection via automatic gain control, *Navigation*, vol.59, no.4, pp.281-290, 2012.