Research Article

Dynamic Search Mechanism with Threat Prediction in a GNSS Receiver

Fang Liu and Meng Liu

School of Information Science and Engineering, Shenyang Ligong University, Shenyang 110159, China

Correspondence should be addressed to Fang Liu; zhqing1019@163.com

Received 8 November 2016; Accepted 12 March 2017; Published 23 March 2017

Academic Editor: Rajesh Khanna

Copyright © 2017 Fang Liu and Meng Liu. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

With the development of GNSS and the application of multimode signals, efficient GNSS receiver research has become very important. However, threat signals in the received signal are inevitable, which will represent important threats to navigation applications and will lead to leakage and fault detection for the receiver. Therefore, the searches with threat prediction in GNSS signals have been regarded as the important problem for GNSS receivers. In view of the limitations and nonadaptability of the current search technologies as well as on the basis of the proportionality peak judgment mechanism, a dynamic search mechanism with threat prediction (DSM-TP) is proposed in this paper, in which we define a series of preset coefficients and a threat index to optimize the decision mechanism. The simulation results demonstrate that the DSM-TP method can predict the threat situation and can adapt to lower SNR environments compared to the traditional method. In addition, the DSM-TP method can avoid the impact of threats, and the detection capability of the new method is better than the detection capability of the traditional method.

1. Introduction

Global navigation satellite systems (GNSS) [1, 2], which include global positioning system (GPS), GALILEO, GLONASS, and COMPASS [3], are currently consolidated and fundamental in satellite communication and mobile communication. GNSS receivers [4] process signals transmitted from satellites to determine user position, velocity, and time. However, to achieve the correct signal reception, it is necessary to determine whether the effective signal exists by using the search detection process. In GNSS, to enhance antijamming and antispoofing capabilities, the longer PRN codes are required. Due to the appearance of long code, the new requirements have been created for the search technology.

Since the clock between transmitter and receiver is different, the local code and received signal may not overlap in time; that is, there is no correlation; thus the search time is uncertain. Additionally, the complexity of the communication channel leads to complexity of the received signal, especially in the conditions of poor environment, human interference, and other threat environments. When there are threat signals in the received signals, the GNSS receiver will

be harmed, especially if the signals are counterfeit [5]. Counterfeit signals have a certain purpose: to provide incorrect information to the target receiver. Examples of incorrect information include incorrect navigation messages and incorrect pseudoranges. This can cause the receiver to output incorrect positions or timing information. Thus, counterfeit signals and jamming signals represent an important threat to navigation applications, and the receiver will also output leakage detection, fault detection, and other issues, especially in fields related to the livelihood of a person such as the military, electricity generation, and finance. Therefore, the search and threat prediction of GNSS signals has become an important problem for GNSS receivers.

In recent years, a series of methods have emerged to meet the demand of efficient GNSS signals search. Transformation domain techniques, such as fast Fourier transform- (FFT-) based methods, are commonly used to reduce acquisition times [6, 7]. In addition, aided search schemes through wireless communication networks or other on-board sensors have been proposed to effectively reduce the search space and decrease the search time [8]. Another known method to explore the amplitude-domain freedom is to construct the

hypercode by superposing several folded segments of the original code [9].

Then, CCPAZP-FFT (Circular Correlation by Partition and Zero Padding) [10] is proposed, which is based on the storage and zero padding segmentation correlation. This algorithm converts two-dimensional searches of time and frequency to one-dimensional search to improve the acquisition efficiency. However, the algorithm is time-consuming in the uncertain code segment by piecewise searching.

XFAST (Extended Replica Folding Acquisition Search Technique) [11, 12] with average input and local samples (direct average) [13] is proposed. This method reduces the amount of computation for direct acquisition but introduces noise during the superposition process. When an increased number of blocks or samples are folded or summed for averaging, the codes result in single correlations more often. Additionally, when more noise is superimposed and included in the correlation results, detection probability decreases. Increased time for folding or summation also results in increased peak position ambiguity, hence lengthening the mean acquisition time. To overcome these problems, a dual-channel method [14] and dual-folding approach (DF-XFAST) [15] are proposed. To achieve the better SNR, this method suggests folding input samples into blocks before undergoing the XFAST operation, which is essentially equivalent to coherent integration of the XFAST correlation results to achieve additional gain.

In addition, to improve the processing speed, the time-frequency domain combination method [16] and frequency domain parallel method [17] are introduced. In these methods, multichannel parallel processing in the time domain and the frequency domain is performed to improve the search speed. However, in the high-dynamic case, the search efficiency of the methods needs to be improved, and due to the influence of the sampling interval, this series of methods still has the limitation of a high missed detection probability. Although the above methods can improve the search speed, they do not have the ability to suppress and predict complex environments and human threat. Therefore, because of the limitations and nonadaptability of the current technologies, a dynamic search mechanism with threat prediction (DSM-TP) is proposed in this paper.

2. Potential Threat Analysis

The signal not only is affected by noise and multipath of the natural environment but also may be artificially unconscious or have conscious malicious damage. For the GNSS receiver, the synchronous search based on the correlation operation is the core; hence, the effect of the correlation operation is the crucial aspect of synchronous search. Therefore, we analyze potential threat signals from the perspective of the impact of related operations.

Although the communication quality can be improved and the threat can be avoided through the frequency escape or jump of the spread frequency signal, in special cases, there may be threat signals in the communication channel. When there are threat signals in the communication channel, threat signals usually form from the spectrum form of GNSS signals, energy concentration region, and correlation characteristic.

FIGURE 1: Threat signal of partial frequency band.

FIGURE 2: Related search influence sample.

The effective energy of the signal may be concentrated in a certain area; therefore, the larger threat is the partial band signal near the center frequency, as shown in Figure 1. When the threat signal frequency covers the center region of the frequency spectrum, signals are most likely to enter the correlator, and when the threat signal energy increases, it may affect correct search of the GNSS signal. A sample of the related search influence is shown in Figure 2. In addition, the influence of the GNSS signal search element is associated with the correlation function of the threat signal. A sample of a threat signal with correlation characteristic is shown in Figure 3. If there is a deviation in the spectrum coverage area, provided that there is partial correlation between the threat signal and the real signals, there is likely a large impact on the search of GNSS signals through the power adjustment. The possible related search effects are shown in Figure 4. If there is no threat analysis and prediction mechanism in the synchronous search, the related decision may fail, which reduces the synchronous receiving efficiency. The threat signal can also be regarded as the real signal, which can cause a significant influence of error application.

FIGURE 3: Threat signal with correlation characteristic.

FIGURE 4: Related search influence sample.

3. Dynamic Search Mechanism with Threat Prediction

For communication signals, the most effective search detection methods use data processing that is based on data segments and FFT. The search decision mechanism is primarily based on relative peak comparison, which is described as traditional method in this paper. Firstly, the received signal is sampled and filtered, and then the local code is generated, extended, and averaged, and another processing is performed to improve the search speed. Then, the frequency estimation error is reduced by multichannel frequency compensation. Furthermore, a multichannel FFT correlation operation is performed between the multiprocessed local and received sequences, and the correlation results are used to calculate the peak value and the average peak value. Finally, a comparison between the maximum peak value and the average peak value is compared with the decision threshold. If the result is successful, the results are output; otherwise, return to the first step, and the signal is rereceived.

Considering the possible drawbacks of the simple absolute energy decision, the decision mechanism uses a proportional peak. Therefore, the proportional peak is defined as

the ratio of the maximum peak and average peak. At the same time, the proportional decision mechanism is defined, which compares the proportional peak and the threshold. The proportional peak is expressed as $P = P_{\max}/P_{\text{ave}}$, in which $P_{\max}$ is the maximum peak energy and P_{ave} is the average peak energy. The effects on $P_{\max}$ and P_{ave} are equal, despite a strong or weak mixed signal; thus the proportional decision mechanism is more suitable for acquisition decision in complex environments. The theory of the proportional decision mechanism is shown in Figure 5.

Based on the proportionality peak judgment mechanism, the decision mechanism is further optimized by considering the influence of a complex environment and threat signals. We define a series of preset coefficients and the threat index, so that a dynamic search mechanism with threat prediction (DSM-TP) is established. The overall flow of DSM-TP is shown in Figure 6.

Step 1. The received branch is selected and updated. And the received signal $S(n)$ is defined as

$$S(n) = d(n) C(n) \cos(\omega n + \theta), \quad (1)$$

where $d(n)$ is the navigation data, $C(n)$ is the pseudocode sequence, ω is the carrier frequency, and θ is the carrier phase.

Step 2. The parameters are initialized. Q_i is initialized using the number of samples N_0 of a chip, in which $i \in [1, 2 \cdots N_0]$. The preset coefficient K is set equal to 1, and the residing coefficient T is set equal to 0.

Step 3. The received signal of the selected branch is sequentially accumulated, and filter processing and front-end processing are performed; then the result sequence is denoted as $S_R(n)$.

$$\begin{aligned} S_R(n) &= \text{fil}[S(n) \cos(\omega_0 n + \theta_0)] \\ &= \text{fil}[d(n) C(n) \cos(\omega n + \theta) \cos(\omega_0 n + \theta_0)] \\ &\approx d(n) C(n) \cos(\Delta\omega n + \Delta\theta), \end{aligned} \quad (2)$$

where $\text{fil}[\]$ is the low-pass filter processing function, ω_0 is the local carrier frequency, θ_0 is the local carrier phase, $\Delta\omega$ is the result carrier frequency, and $\Delta\theta$ is the result carrier phase.

Step 4. It is determined if the T value is equal to or greater than 5. If the condition is satisfied, Step 19 is executed; otherwise, go back to Step 5.

Step 5. The local pseudocode sequence $C_{Li}(n)$ is generated; then the data result of mean processing and spread processing is denoted as $S_L(n)$.

$$S_L(n) = \sum_{i=1}^M C_{Li}(n). \quad (3)$$

Step 6. The correlation operation is performed between $S_R(n)$ and $S_L(n)$, and the result is denoted as $V(n)$.

$$\begin{aligned} V(n) &= S_R(n) * S_L(n) \\ &= \text{abs}[\text{IFFT}[\text{FFT}(S_R(n)) \cdot \text{FFT}^*(S_L(n))]]. \end{aligned} \quad (4)$$

FIGURE 5: The proportional decision mechanism.

Step 7. The peak values are calculated using the correlation results $V(n)$, and the maximum peak is denoted as V_m , and the average peak is denoted as V_v , where L is the length of $V(n)$.

$$\begin{aligned} V_m &= \max [V(n)], \\ V_v &= \frac{\sum V(n)}{L}. \end{aligned} \quad (5)$$

Step 8. The threshold factor is calculated using $V(n)$, V_m , and L .

$$\xi = \frac{\sum V(n)}{\sum V(n) - V_m} \cdot \frac{L-1}{L}. \quad (6)$$

Step 9. The threshold is calculated as $G = \xi \cdot V_v$.

Step 10. The parameter N is defined and set equal to 0; then N is described as

$$N = \begin{cases} N+1, & \text{if } V(n)|_1^L > G \\ N, & \text{other,} \end{cases} \quad (7)$$

where $V(n)|_1^L$ is the traverse function from $V(1)$ to $V(L)$.

Step 11. The removal function $\chi[\]$ is defined. It expresses that b position sequence is removed from $V(n)$, which is described as

$$\begin{aligned} \chi[V(n), b] \\ = \{V(1), V(2) \cdots V(b-1), V(b+1), \dots, V(L)\}. \end{aligned} \quad (8)$$

Then, P_i is defined, whose initial value is equal to 0; $i \in [1, 2 \cdots N]$. And the maximum position function $\max_i[\]$ is defined. It expresses the position of the N th largest peak in $V(n)$, which is described as

$$\begin{aligned} P_i &= \max_i [V(n)] = \max \{\chi[V(n), P_{i-1}]\} \\ &= \max \{V(1), V(2) \cdots V(P_{i-1}-1), V(P_{i-1}+1), \dots, \\ &V(L)\}. \end{aligned} \quad (9)$$

Thus, $P_1, P_2, \dots, P_N$ can be obtained. An example is used to calculate P_i , which is shown in Figure 7.

Step 12. It is determined if the N value is greater than 1. If the condition is satisfied, Step 13 is executed; otherwise, go to Step 14.

Step 13. It is determined if the N value is equal to 1. If the condition is satisfied and the preset coefficient is adjusted as $K = K + 1$, then Step 16 is executed; otherwise, the new signal is rereceived, and the parameters are adjusted; then go back to Step 1.

Step 14. It is determined if the N value is greater than N_0 . If the condition is satisfied, the new signal is rereceived, and the parameters are adjusted, then go back to Step 1; otherwise, go to Step 15.

Step 15. P_i and cache variables Q_i are compared under branching conditions.

$$\begin{aligned} K &= K + 1, & \text{if } P_1 == Q_1 \\ \lambda &= \lambda + 1, & \text{if } P_{\text{other}} == Q_{\text{other}} \\ K &= K - 1, & \text{if } P_1 == Q_{\text{other}}, \text{ or } P_{\text{other}} == Q_1. \end{aligned} \quad (10)$$

Step 16. It is determined if the K value is greater than 1. If the condition is satisfied, this branch signal is continually received, and the residing coefficient is adjusted as $T = T + 1$, then go back to Step 3; otherwise, go to Step 17.

Step 17. Then, Q_i is updated using P_i .

Step 18. It is determined if the K value is greater than 3. If the condition is satisfied, Step 19 is executed; otherwise, this branch signal is continually received, and the residing coefficient is adjusted as $T = T + 1$; then go back to Step 3.

Step 19. The acquisition position parameter P is output and the potential threat index W is analyzed.

$$\begin{aligned} P &= \begin{cases} P = Q_1; & \text{if } K = 3 \\ P = \text{error}; & \text{if } K \neq 3, \end{cases} \\ W &= \begin{cases} W = 1; & \text{if } \lambda = 0 \\ W = 2; & \text{if } \lambda = 1 \\ W = 3; & \text{if } \lambda > 1. \end{cases} \end{aligned} \quad (11)$$

FIGURE 6: Overall flow of DSM-TP.

When W is equal to 1, it indicates that there are no man-made threats in the received signals. When W is equal to 2, it indicates that there may be man-made threats in the received signals, but there are no correlation characteristics between

the threat signals and the real signal. When W is equal to 3, it indicates that there are man-made threats in the received signals, and there are correlation characteristics between the threat signals and the real signal.

FIGURE 7: The calculated process of P_i .

FIGURE 8: Proportion peak for changing SNR.

4. Test and Analysis

4.1. Analysis under Safe Conditions. Based on the simulation platform, the DSM-TP method and the traditional method are tested when the receiver is in a safe environment. Input parameters are as follows: BPSK modulation, a signal bandwidth of 10 MHz, and proportional threshold equal to 10. For different values of SNR, the DSM-TP method and the traditional method are tested, and the proportion peak results are shown in Figure 8. For the same SNR value, the correlation result of the new method is superior to the traditional method. For a threshold equal to 10, the effective SNR of the new method is greater than -17 dB, while the conventional method is larger than -14 dB, indicating that SNR adaptability of the new method is better than the traditional method. Further, the detection probability of each method is shown in Figure 9 for different SNR values. For

TABLE 1: Threat prediction results of the two methods.

SNR	Method	
	DSM-TP method	Traditional method
10 dB	Correctly; $w = 1$, predict nonthreat state	Correctly; No prediction
0 dB	Correctly; $w = 1$, predict nonthreat state	Correctly; No prediction
-14 dB	Correctly; $w = 1$, predict nonthreat state	Incorrectly; No prediction
-17 dB	Alarm and rereceive; $w = 1$, predict nonthreat state	Incorrectly; No prediction

FIGURE 9: Detection probability for changing SNR.

the same SNR condition, the detection probability of the new method is greater than that of the traditional method, indicating that the detection capability of the new method is better than that of the traditional method.

The results of threat prediction ability for the two methods are shown in Table 1. When the SNR is greater than -17 dB, the new method can search correctly and predicts that there are no man-made threats present in the environment, which agrees with the actual input situation. When the SNR is less than -17 dB, the alarm is issued and a research is performed. It also predicts no man-made threats to be present in the environment. However, the traditional method can search correctly when the SNR is greater than -14 dB but cannot predict the threat. When the SNR is less than -14 dB, the traditional method cannot search correctly and cannot predict the threat. This indicates that the new method can adapt to lower SNR environments compared to the traditional method and also predicts the threat situation.

FIGURE 10: Proportion peak for changing S/J .

4.2. Analysis under Partial Frequency Band Threat Conditions.

The DSM-TP method is tested when the receiver is in a threat environment. Input parameters are as follows: BPSK modulation, signal bandwidth equal to 10 MHz, and proportional threshold equal to 10. Let the form of the threat signals be the uniform spectrum interference, whose frequency is in the center frequency, and the spectrum covers 80% of the main frequency band of the real signal. Let S/J be the ratio of the real signal energy and the threat signal energy, and the larger the S/J value, the less the relative energy of jamming. For different S/J values, the DSM-TP method and the traditional method are tested, and the proportion peak results are shown in Figure 10. When S/J is equal to 0, that is, the energies of the real signal and the threat signal are equal, the correlation value of the new method is greater than that of the traditional method: 30 dB. For a threshold value equal to 10, effective S/J of the new method is larger than -28 dB, while the conventional method is larger than -21 dB, indicating that S/J adaptability of the new method is better than the traditional method. Furthermore, for changes in the S/J value, the detection probability of each method is shown in Figure 11. For the same S/J conditions, the detection probability of the new method is greater than the detection probability of the traditional method, indicating that the detection capability of the new method is better than that of the traditional method.

The results of the threat prediction ability of the two methods are shown in Table 2. When S/J is greater than -28 dB, the new method searches correctly. It can predict that the potential threat index W is equal to 2, which verifies that there are man-made threats in the environment, but there is not a correlation characteristic between the threat signals and the real signal. When the SNR is less than -28 dB, the alarm is issued and a research is performed. It can predict that there are man-made threats in the environment, but there is not a correlation characteristic between the threat

TABLE 2: Results of threat prediction for the two methods.

J/S	Method	
	DSM-TP method	Traditional method
25 dB	Correctly; $w = 2$, predict threat state but no correlation	Correctly; No prediction
15 dB	Correctly; $w = 2$, predict threat state but no correlation	Correctly; No prediction
0 dB	Correctly; $w = 2$, predict threat state but no correlation	Correctly; No prediction
-21 dB	Correctly; $w = 2$, predict threat state but no correlation	Incorrectly; No prediction
-28 dB	Alarm and rereceive; $w = 2$, predict threat state but no correlation	Incorrectly; No prediction

FIGURE 11: Detection probability for changing S/J .

signals and the real signal. The results are consistent with the actual input situation. However, the traditional method can search correctly when the SNR is larger than -21 dB, but it cannot predict the threat. When the SNR is less than -21 dB, the traditional method cannot search correctly and cannot predict the threat. These results indicate that the new method can adapt to a threat environment better than the traditional method and can also predict the threat situation.

4.3. Analysis under Correlation Characteristic Threat Conditions.

The DSM-TP method is tested when there is correlation characteristic between the threat signals and the real signal, and the pseudocode overlap rate of the threat signal and real signal is set to 30%. For different S/J values, the DSM-TP method and the traditional method are tested, and the

FIGURE 12: Proportion peak for changing S/J . FIGURE 14: Proportion peak for changing S/J . FIGURE 13: Detection probability for changing S/J . FIGURE 15: Detection probability for changing S/J .

proportion peak results are shown in Figure 12. When S/J is equal to 0, the correlation value of the new method is greater than the value of the traditional method, 20 dB. For the same S/J conditions, the correlation result of the new method is superior to the traditional method. However, when S/J is less than -10 dB, the new method has a very low correlation peak and does not meet the threshold requirement. Thus, the receiver is determined to be in a threat environment, and then the signal is rereceived. However, when S/J is less than -10 dB, the correlation peak of the traditional method is larger and meets the threshold requirements. Although the receiver is considered to be secure, the threat signal is received and misinterpreted as a real signal in the traditional method. These results indicate that the new method can search correctly under the relevant threat condition and avoid the false threat. Further, for different values of S/J , the detection probability of each method is shown in Figure 13. Under

the effective S/J condition, the detection probability of the new method is greater than the detection probability of the traditional method, indicating that the detection capability of the new method is better than the traditional method.

Furthermore, the DSM-TP method is tested when the pseudocode overlap rate of threat signal and real signal is set to 50%, with the proportion peak results shown in Figure 14 and the detection probability shown in Figure 15. For a pseudocode overlap rate of the threat signal and real signal equal to 80%, the proportion peak results are shown in Figure 16, and the detection probability is shown in Figure 17. These results indicate that as the pseudocode overlap rate increases, the S/J values of the correlation results that do not satisfy the threshold requirement decrease, indicating that as the pseudocode overlap rate increases, the threat of interference increases. Although the impact of this threat is

TABLE 3: Threat prediction results of the two methods.

Overlap rate and J/S		Method	
		DSM-TP method	Traditional method
30%	20 dB	Correctly; $w = 3$, predict threat state and correlation	Correctly; No prediction
	0 dB	Correctly; $w = 3$, predict threat state and correlation	Correctly; No prediction
	-10 dB	Alarm and rereceive; $w = 3$, predict threat state and correlation	Spoofing; No prediction
50%	20 dB	Correctly; $w = 3$, predict threat state and correlation	Correctly; No prediction
	0 dB	Correctly; $w = 3$, predict threat state and correlation	Correctly; No prediction
	-5 dB	Alarm and rereceive; $w = 3$, predict threat state and correlation	Spoofing; No prediction
80%	20 dB	Correctly; $w = 3$, predict threat state and correlation	Correctly; No prediction
	0 dB	Alarm and rereceive; $w = 3$, predict threat state and correlation	Spoofing; No prediction

FIGURE 16: Proportion peak for changing S/J . FIGURE 17: Detection probability for changing S/J .

large, the new method can also predict the existence of the threat and can rereceive the signals. However, the traditional method will mistakenly receive the threat signal, and the threat signal is erroneously treated as a real signal. These results indicate that the new method can search correctly under the relevant threat conditions and avoid the false threat, and the detection capability of the new method is better than the traditional method under the effective S/J condition.

The results of threat prediction for the two methods are shown in Table 3 for pseudocode overlap rates of the threat signal and real signal equal to 30%, 50%, and 80%. When S/J is greater than -10 dB, -5 dB, and 0 dB, under different overlap

rate conditions, the new method can search correctly. It can predict that the potential threat index W is equal to 3, which verifies that there are man-made threats in the environment and there is a correlation characteristic between the threat signals and the real signal. When S/J is less than -10 dB, -5 dB, and 0 dB, under different overlap rate conditions, the alarm is issued and a research is performed. It can predict that there are man-made threats in the environment and there is a correlation characteristic between the threat signals and the real signal. The results are consistent with the actual input situation. However, the traditional method can search correctly when S/J is greater than -10 dB, -5 dB, and 0 dB, under different overlap rate conditions, but it cannot

predict the threat. When S/J is less than -10 dB, -5 dB, and 0 dB, under different overlap rate conditions, the traditional method is affected by the false threat and cannot predict the threat. These results indicate that the new method can adapt to the false threat environment better than the traditional method and can also predict the false threat.

5. Conclusions

In view of the limitations and nonadaptability of current search technology, the proportionality peak judgment mechanism is further optimized considering the influence of complex environment and threat signals. A dynamic search mechanism with threat prediction is proposed, in which we define a series of preset coefficients and a threat index. The simulation results demonstrate that the new method can adapt to lower SNR environments compared to the traditional method in safe conditions, and the detection probability of the new method is higher than the detection probability of the traditional method. Furthermore, these methods are tested in threat conditions, and the results demonstrate that the new method can adapt to the threat environment better than the traditional method and can also predict the threat situation and predict the spoofing threat. In addition, the detection capability of the new method is better than the traditional method in safe conditions and threat conditions.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (no. 61501309) and the China Postdoctoral Science Foundation (no. 2015M580231).

References

- [1] J.-C. Juang and Y.-H. Chen, "Global navigation satellite system signal acquisition using multi-bit codes and a multi-layer search strategy," *IET Radar, Sonar and Navigation*, vol. 4, no. 5, pp. 673–684, 2010.
- [2] P. B. S. Harsha and D. V. Ratnam, "Implementation of advanced carrier tracking algorithm using adaptive-extended kalman filter for GNSS receivers," *IEEE Geoscience and Remote Sensing Letters*, vol. 13, no. 9, pp. 1280–1284, 2016.
- [3] D. H. Xia, C. H. Liu, Z. J. Wang et al., "Reconstruction progress of the COMPASS-D ECRH system on J-TEXT," *IEEE Transactions on Plasma Science*, vol. 44, no. 9, pp. 1649–1653, 2016.
- [4] L. Lestarquit, M. Peyrezabes, J. Darrozes et al., "Reflectometry with an open-source software GNSS receiver: use case with carrier phase altimetry," *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, vol. 9, no. 10, pp. 4843–4853, 2016.
- [5] J. Li, J. Zhang, S. Chang, and M. Zhou, "Performance evaluation of multimodal detection method for GNSS intermediate spoofing," *IEEE Access*, vol. 4, pp. 9459–9468, 2016.
- [6] D. Akopian, "Fast FFT based GPS satellite acquisition methods," *IEEE Proceedings—Radar, Sonar and Navigation*, vol. 152, no. 4, pp. 277–286, 2005.
- [7] J. B. Y. Tsui, *Fundamentals of Global Positioning System Receivers: A Software Approach*, John Wiley & Son, New York, NY, USA, 2000.
- [8] J. B. Bullock, M. Foss, G. J. Geier, and M. King, "Integration of GPS with other sensors and network assistance," in *Understanding GPS Principles and Applications*, Artech House, Boston, Mass, USA, 2006.
- [9] A. R. A. Moghaddam, R. Watson, G. Lachapelle, and J. Nielsen, "Exploiting the orthogonality of L2C code delays for a fast acquisition," in *Proceedings of the Institute of Navigation—19th International Technical Meeting of the Satellite Division (ION GNSS '06)*, pp. 1233–1241, Fort Worth, Tex, USA, September 2006.
- [10] Y. Wei, *GPS Spread Spectrum Code Synchronization Technology Research*, University of Electronic Science and Technology of China, Chengdu, China, 2007.
- [11] Y. Ren, W. Peng, W. Xu, and X. Wang, "The research progress of direct acquisition technology of GPS P(Y)-code," *Global Positioning System*, vol. 2, pp. 2–9, 2003.
- [12] C. Yang, J. Vasquez, and J. Chaffee, "Fast direct P(Y)-code acquisition using XFAST," in *Proceedings of the 12th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GPS '99)*, pp. 317–324, Nashville, Tenn, USA, September 1999.
- [13] Q. Zeng, L. Tang, P. Zhang, and L. Pei, "Fast acquisition of L2C CL codes based on combination of hyper codes and averaging correlation," *Journal of Systems Engineering and Electronics*, vol. 27, no. 2, pp. 308–318, 2016.
- [14] W. Feng, X. Xing, Q. Zhao, and Z. Wang, "Dual-channel method for fast long PN-code acquisition," *China Communications*, vol. 11, no. 5, pp. 60–70, 2014.
- [15] H. Li, X. Cui, M. Lu, and Z. Feng, "Dual-folding based rapid search method for long PN-code acquisition," *IEEE Transactions on Wireless Communications*, vol. 7, no. 12, pp. 5286–5296, 2008.
- [16] F. Liu and Y. Feng, "A fast acquisition algorithm overcoming fuzz problems for TDDM spread spectrum signal," *Mathematical Problems in Engineering*, vol. 2014, Article ID 362061, 12 pages, 2014.
- [17] F. Liu and Y. Feng, "A long code acquisition algorithm on resolve time-frequency uncertainty problem," *Acta Aeronautica et Astronautica Sinica*, vol. 34, no. 8, pp. 1924–1933, 2013.