An BDS Spoofing Interference Detection and Identification Method Using the Radio Determination Satellite Service

Zhengkun Chen, Jing Li, Qizhen Weng, Fan Feng, Du Li, Xuelin Yuan, Xiangwei Zhu
School of Electronics and Communication Engineering
Sun Yat-Sen University
Shenzhen, China
chenzhk8@mail2.sysu.edu.cn, zhuxw666@mail.sysu.edu.cn

***Summary*—The vulnerability of the BeiDou navigation satellite system (BDS) to potential spoofing interference poses a significant challenge to its widespread application in transportation, power timing, and other industries. How to detect and identify spoofing interference rapidly and exactly becomes a critical issue. The traditional receiver autonomous integrity monitoring (RAIM) can detect and identify a few spoofed satellites through the consistent detection of redundant observations, while it will be ineffective in the case of most satellites being spoofed. This paper proposes a spoofing BDS interference detection and identification method using radio determination satellite service (RDSS) pseudo-range assistance. The signal of BDS RDSS has a two-way user authentication system at the master station, which is challenging to be spoofed. Using the RDSS pseudo-range observation to provide additional information for the RAIM algorithm can enhance the fault detection and identification capability. The simulation results show that the RDSS-assisted method can still effectively detect and identify spoofed interfering satellites in the case of the majority of satellites being spoofed, and the availability of the proposed method is significantly improved over the traditional RAIM method.**

Keywords—BDS; radio determination satellite service; spoofing interference; detection and identification; receiver autonomous integrity monitoring

I. INTRODUCTION

Since its fully deployment in 2020, the BeiDou satellite navigation system (BDS) has been widely utilized in various fields such as transportation, power timing, and public security due to its high accuracy and diverse services[1]. However, the general vulnerability of radio navigation satellite service (RNSS) to potential threats of spoofing interference has also limited its application in some critical areas, and studies have shown that RNSS spoofing interference can cause positioning and timing failure [2]. As a result, identifying and detecting RNSS spoofing interference rapidly and accurately has become a crucial challenge.

The traditional receiver autonomous integrity monitoring (RAIM) can detect and identify the spoofed satellites through the consistent detection of redundant observations. However, it may not work when most or even all satellites are spoofed. Reference [3] proposed a one-dimensional traversal maximum likelihood estimation MLE-RAIM method for anti-spoofing applications, which can exclude multiple spoofing signals, but it requires significant computing resources. Another approach is to use additional sensors such as IMUs and high-precision clocks to provide auxiliary information for spoofing interference detection [4]-[5]. Reference [4] proposed a measurement deviation determination method that can successfully avoid spoofing with tightly-coupled GNSS/IMU. However, it may significantly increase user costs.

The BDS-3 system offers standard RNSS services, enabling users to access reliable satellite communication and PVT services [2]. Dual-mode receiver products supporting both RNSS and RDSS services are already available at relatively low cost. The RDSS signal incorporates a two-way user authentication system at the master station, making it resilient to spoofing interference. Reference [6] proposes an anti-spoofing technology in the location domain using comprehensive RDSS service, and a classifier of RNSS pseudo-range is constructed using RDSS pseudo-range. However, this approach requires the receiver to have a multi-peak acquisition and tracking architecture. In this paper, the RDSS pseudo-range observation volume is utilized to provide additional reference information for the RAIM algorithm, which can improve the fault detection and identification capability, combining the high reliability of RDSS and the high precision of RNSS.

II. METHODS

A. The Principle of *BDS RNSS and RDSS Services*

The schematic diagram of the two services of the BDS is shown in Fig. 1, where the solid blue line indicates the standard RNSS signal, which can be broadcasted by the geostationary orbit (GEO), medium earth orbit (MEO) and inclined geosynchronous orbit (IGSO) satellites; the blue dashed line indicates the RNSS spoofing signal broadcasted by the timing spoofing simulator; the red line indicates the RDSS signal of the BDS. The signal transmitted from the master control center (MCC) and forwarded to a user via a GEO satellite is called the outbound signal. The signal transmitted by a user and forwarded to the master station via a GEO satellite is called the inbound signal. The outbound and inbound signals are denoted

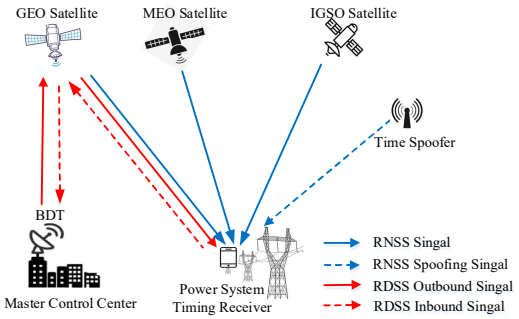

Fig. 1. Diagrams of the RNSS and RDSS satellite timing and spoofing interference in the BDS.

by solid red lines and red dashed lines, respectively. These types of satellites can be used for the timing of a power system.

For RNSS positioning, the RNSS pseudo-range equation between the ith satellite and the receiver can be expressed as

$$\rho_i = \sqrt{(x_i - x_u)^2 + (y_i - y_u)^2 + (z_i - z_u)^2} + c(t_u - t_i) + \varepsilon_i \quad (1)$$

where (x_i, y_i, z_i) is the location of the ith satellite, (x_u, y_u, z_u) is the location of the receiver, t_u is the receiver clock overrun relative to system time, t_i is the overrun of the clock of the ith satellite relative to system time, ε_i is the pseudo-range measurement error of the ith satellite. Knowing the pseudo-range and ephemeris of at least 4 satellites, the user's position and time information can be solved by listing a system of equations.

The BeiDou RDSS positioning system consists of two geostationary satellites, a user, and a measurement control center(MCC), and operates on the principle of calculating the pseudo-range by transmitting a measurement signal from the user to the satellite and then to the MCC. The two-way transmission time from the user to the MCC via the satellite is then added to calculate the user's geographic elevation in the elevation library stored in the MCC, which is used to determine the user's coordinates. The MCC then sends the user's coordinate information to the user via the satellite, thereby completing the positioning service.

Assuming that the jth satellite is a GEO satellite, similar to the RNSS pseudo-range, the RDSS pseudo-range can be expressed as a two-way pseudo-range from the MCC to the satellite and then to the user:

$$l_j = 2 * \{\left[(x_0 - x_j)^2 + (y_0 - y_j)^2 + (z_0 - z_j)^2\right]^{\frac{1}{2}} + \left[(x_u - x_j)^2 + (y_u - y_j)^2 + (z_u - z_j)^2\right]^{\frac{1}{2}}\} + c(t'_u - t_i) + \eta_i \quad (2)$$

where (x_0, y_0, z_0) is the location of the MCC. The first term in the equation is the pseudo-range measurement from the MCC to the satellite, and the second term is the pseudo-range measurement from the satellite to the user. t'_u is the receiver clock overrun relative to system time, t_i is the overrun of the clock of the ith satellite relative to system time, same as RNSS system, η_i is the pseudo-range measurement error of the ith satellite.

B. *RAIM-based spoofing detection and identification method for RNSS*

Receiver Autonomous Integrity Monitoring (RAIM) was originally designed as a terminal signal processing method to detect and identify faults. Since spoof signals can lead to erroneous measurements, RAIM can be extended to the field of spoof detection and can treat spoof signals as fault signals. RAIM can detect faults and troubleshoot only one fault by testing the consistency of measurements from various satellites. However, when multiple spoof signals are present at the same time, and it is necessary to filter the visible satellites to achieve spoof identification by a subset of consistency checks.

The RAIM algorithm requires at least five visible satellites to achieve spoof detection, and the commonly used methods are the least squares residuals method and the parity space method [7]. This paper focuses on spoof detection and identification based on the least squares residuals method.

Knowing the pseudorange of at least four visible satellites, the four unknown quantities $[x, y, z, \delta t_u]$ can be solved, where δt_u is the receiver clock difference which equals ct_u.

With m visible satellites, the GNSS observation equation after associating multiple pseudo-range equations and linearizing them can be expressed as:

$$\begin{bmatrix} f_x^1(x) & f_y^1(y) & f_z^1(z) & 1 \\ f_x^2(x) & f_y^2(y) & f_z^2(z) & 1 \\ \vdots & \vdots & \vdots & \vdots \\ f_x^K(x) & f_y^K(y) & f_z^K(z) & 1 \end{bmatrix} \begin{bmatrix} \Delta x_u \\ \Delta y_u \\ \Delta z_u \\ c\Delta\delta t_u \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_K \end{bmatrix} \quad (3)$$

$$f_x^i = \frac{x_u - x_i}{r_i}, f_y^i = \frac{y_u - y_i}{r_i}, f_z^i = \frac{z_u - z_i}{r_i}$$

$$r_i = [(x_u - x_i)^2 + (y_u - y_i)^2 + (z_u - z_i)^2]^{1/2}$$

$$g_x^i = f_x^i, g_y^i = f_y^i, g_z^i = f_z^i$$

$$b_i = \rho_i - r_i - c\delta t_u, v_i = l_i/2 - r_j$$

Simplify the above equation we have:

$$\boldsymbol{Z} = \boldsymbol{HX} + \boldsymbol{\varepsilon} \quad (4)$$

where the vector $\boldsymbol{Z}$ is the difference between the measured pseudo-range and the estimated pseudo-range, which is obtained by incorporating the receiver approximate position and clock deviation into the pseudo-range equation. The measured value is the pseudo-range measurement obtained by the receiver. The matrix $\boldsymbol{H}$ is the design matrix, while $\boldsymbol{X}$ is the estimated state vector, which comprises three position components and the receiver clock deviation for the same source, three position components, RNSS clock deviation and RDSS clock deviation for different sources. Finally, the vector $\boldsymbol{\varepsilon}$ is the $N \times 1$ observation noise vector.

According to the least squares algorithm, the estimation of $\boldsymbol{X}$ is:

$$\hat{\boldsymbol{X}} = (\boldsymbol{H}^T\boldsymbol{H})^{-1}\boldsymbol{H}^T\boldsymbol{Z} \quad (5)$$

The pseudo-range residual can be expressed as

$$w = [\boldsymbol{I_n} - \boldsymbol{H}(\boldsymbol{H}^T\boldsymbol{H})^{-1}\boldsymbol{H}^T]\boldsymbol{Z} \quad (6)$$

In the RAIM method, the residual is utilized as a decision variable to determine the presence of outliers in the measurement. The sum of squared residuals can be expressed as:

$$SSE = w^T w \quad (7)$$

Let $D = SSE/\sigma_0^2$ and σ^2 be the variance of the pseudo-range measurement error.

Assuming that the elements of $\boldsymbol{\varepsilon}$ follows a Gaussian distribution with mean zero and variance σ_0^2. In the absence of faults, D follows a chi-squared distribution with degrees of freedom of $N-4$. However, in the absence of faults, it follows a non-central chi-squared distribution.

The detection threshold can be pre-calculated based on the false alarm rate requirement and the number of visible satellites. If N is the number of visible satellites involved in the calculation, then two hypotheses can be formulated: H_0 for fault-free situation and H_1 for situation with faults.

$$H_0:\ D \sim \chi^2(N-4)$$
$$H_1:\ D \sim \chi^2(N-4,\lambda)$$

Therefore, for a given false alarm rate,

$$P(D < \mathrm{T}) = \int_0^T f_{x^2(N-4)}(x)dx = 1 - P_{\mathrm{FA}} \tag{8}$$

The equation can be used to determine the detection threshold T. If D is less than T, it is considered that no spoofing is present; otherwise, it is considered that spoofing has occurred. The non-central parameter λ is related to the size of the error, with larger errors corresponding to larger λ values. Therefore, the threshold T can be adjusted accordingly based on the level of error tolerance and the probability of false alarms, to ensure a reliable and effective spoofing detection system.

After spoofing is detected, it is also possible to identify spoofing satellite by using the observation subset testing method [8],[9].

C. RDSS-assisted RAIM spoofing detection and identification method

When employing least squares residuals RAIM to detect spoofing, a minimum of five visible satellites is required for spoofing detection and six for identifying specific spoofed satellites. In situations where a large number of satellites are spoofed simultaneously, the conventional least squares residuals test method may incorrectly treat the spoofed satellite signals as standard, while classifying normal satellite signals as anomalous satellites. To address this issue, the normal pseudo-range of RDSS provided by the GEO satellites can be utilized as a priori information in conjunction with the least squares residuals method, in order to assess consistency among the satellites.

The following section describes the principle of the RDSS-assisted the least squares residual RAIM algorithm. The difference mainly lies in the design matrix H and the distribution of the residual statistic *D*.

For RNSS and RNSS different clock source systems, if the pseudo-ranges of at least five visible satellites are known, the five unknown quantities $[x, y, z, \delta t_u, \delta t_u']$ can be solved, where δt_u is the RNSS source clock difference of the receiver which equals ct_u, and $\delta t_u'$ is the receiver's RDSS source clock difference which equals ct_u'.

With m visible GEO satellites that can acquire both RNSS and RDSS information and k other visible satellites with RNSS information only, the GNSS observation equation after associating multiple pseudo-range equations and linearizing them can be expressed as follows:

$$\begin{bmatrix} f_x^1(x) & f_y^1(y) & f_z^1(z) & 1 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ f_x^k(x) & f_y^k(y) & f_z^k(z) & 1 & 0 \\ g_x^1(x) & g_y^1(y) & g_z^1(z) & 0 & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ g_x^m(x) & g_y^m(y) & g_z^m(z) & 0 & 1 \end{bmatrix} \begin{bmatrix} \Delta x_u \\ \Delta y_u \\ \Delta z_u \\ \Delta\delta t_u \\ \Delta\delta t_u' \end{bmatrix} = \begin{bmatrix} b_1 \\ \vdots \\ b_k \\ v_1 \\ \vdots \\ v_m \end{bmatrix} \tag{9}$$

$$f_x^i = \frac{x_u - x_i}{r_i}, f_y^i = \frac{y_u - y_i}{r_i}, f_z^i = \frac{z_u - z_i}{r_i}$$
$$r_i = [(x_u - x_i)^2 + (y_u - y_i)^2 + (z_u - z_i)^2]^{1/2}$$
$$g_x^i = f_x^i, g_y^i = f_y^i, g_z^i = f_z^i$$
$$b_i = \rho_i - r_i - c\delta t_u, v_j = l_j/2 - r_j$$

In particular, for RNSS and RDSS simultaneous clock source systems we have $\Delta\delta t_u'$=$\Delta\delta t_u$.

Using the least squares residual method similar to the traditional RAIM to calculate the residual statistic D, there are 5 unknown quantities to be solved, then for fault-free situations and situations with faults, the distribution of D obeys:

$$H_0:\ D \sim \chi^2(n-5)$$
$$H_1:\ D \sim \chi^2(N-5,\lambda)$$

Therefore, for a given false alarm rate P_{FA}, the threshold T can be determined by the following equation:

$$\int_0^T f_{x^2(N-5)}(x)dx = 1 - P_{\mathrm{FA}} \tag{10}$$

To identify spoofing satellites, a subset screening method is commonly used in RAIM. In this method, m visible GEO satellites are used as a priori information and not included in subset screening. In each cycle, h satellites are removed from the remaining k satellites to form C_k^h subsets. Each subset is then used to perform a residual test jointly with RDSS observations. The value of h starts from 1 and increases in each cycle until a subset with residual statistics below the test threshold is screened out and used for subsequent solving. Then the satellites outside the subset are excluded, ensuring that the positioning timing results are not affected by spoofing signals.

D. The Algorithm

In this paper, the normal pseudo-range of RDSS provided by GEO satellites is used as a priori information to perform the least squares residual method with other satellites detected in RAIM consistency detection. The process of RNSS spoofing interference detection based on RDSS assistance is shown in Fig. 1, which mainly consists of five steps:

1) Obtaining the linearized observation equation with RNSS observations and RDSS observations.

2) Solving the PVT solution using the least squares.

3) Computing the residual statistics (D).

4) Definition the test statistic.

5) Comparing with the threshold. If the value of D is greater than the pre-calculated threshold, it is considered that there are spoofing signals present, and further testing is carried

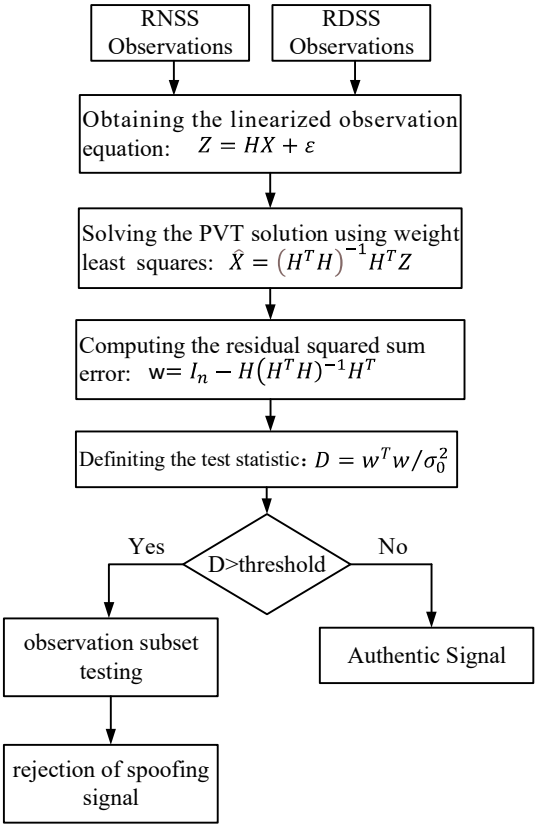

Fig. 2. The flow chart of RDSS-assisted RAIM spoofing detection

out on the subsets of observations to screen out the non-spoofing subsets, thus achieving the rejection of spoofing interference.

III. RESULTS AND DISCUSSION

A. Simulation Platform

The dataset used in this experiment is generated by the signal source with 16 visible satellites, among which GEO satellites are satellites 1-5 that can provide RDSS and RNSS services simultaneously. The Fig. 3. Shows the sky map of the BDS in the receiver's area. This experiment only utilizes the RDSS data of 1 and 2 of these satellites. The total length of the data is 10 minutes , during which a slow drift occurs from the 180th second and it reaches the target clock difference at the 420th second.

Our experiment consists of three main parts: minority spoofing dataset, majority spoofing dataset, and all satellite spoofing dataset. In each part, we compared the performance of Method A, which is the traditional RAIM algorithm, with Method B, which is the RDSS-assisted RAIM algorithm, in detecting and identifying spoofing signals under different scenarios. The detection performance was evaluated using the change feature of the residual statistics, while the identification performance was measured by the clock difference of the final solution. The preset false alarm rate P_{FA} for this experiment is 0.1%.

Table. 1. Signal Source Data Simulation Experiment Scenario Information

Number	Scenario	Number of spoofed satellites	Pull-off time
1	minority spoofing	2	100ns
2	majority spoofing	10	1ms
3	all spoofing	16	100ns

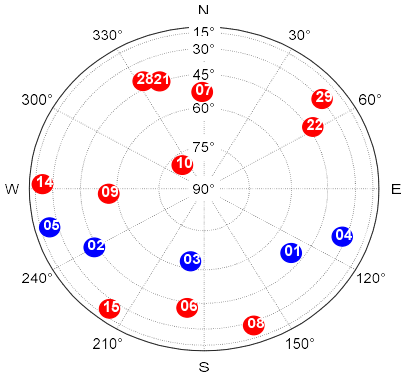

Fig. 3. The sky map of the BDS in the receiver's area

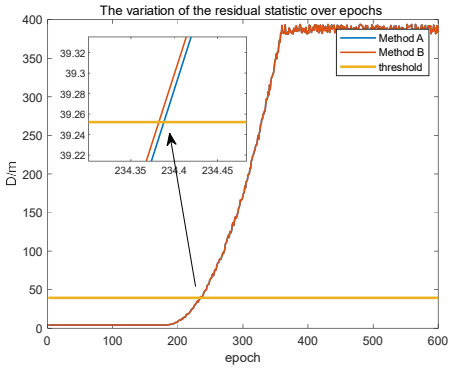

Fig. 4. The change of residual clock difference between the two methods when the 2 satellites are pulled off 100ns

B. Analysis of Experimental Results

Minority spoofing dataset was tested first, and it can be seen from Fig. 4 that the two RAIM algorithms increase to a certain level of residual statistics over the threshold during the slow growth of the pull-off time. The effectiveness of the RAIM algorithm in detecting a small number of satellite spoofing can be demonstrated, and the RDSS-based RAIM algorithm is still effective in this case.

In the majority spoofing scenario, both methods are capable of detecting spoofing signals, but their identification performance judged by the solved clock error differs. Initially, when the pull-off differences is small, both algorithms fail to correctly identify and exclude the spoofed satellite. However, as the pull-off difference increases, the RAIM algorithm assisted by RDSS information successfully identifies the spoofed satellites and excludes them, resulting in the solved clock difference returning to normal values instead of continuing to be pulled off. This indicates that for majority

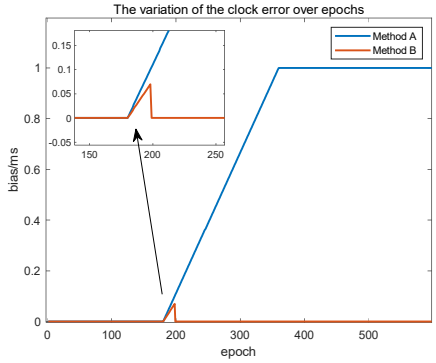

Fig. 5. Variation of the clock difference obtained by the two methods when 10 satellites are pulled off

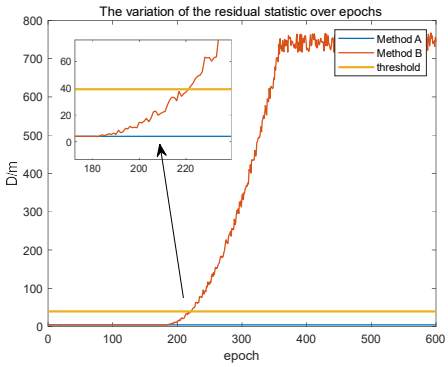

Fig. 6. Variation of residual statistics for all satellite spoofing scenario

spoofing scenarios, the RNSS RAIM method can only detect the spoofing signals, but cannot accurately identify them, while the RDSS-assisted method can achieve correct detection and identification.

When the number of spoofing satellites continues to increase $(> N - 4)$, according to the principle of satellite signal solving, the amount of information from the real satellite signals is no longer sufficient to obtain an accurate solution, leading to position and clock difference shifts. However, it is still possible to focus on the problem of detecting spoofing signals, which can alert the user to the presence of spoofing signals.

The changes of the residual statistics under both methods in the scenario of full satellite spoofing are illustrated in Fig. 6. As observed, the RAIM algorithm that only uses RNSS information does not indicate an increase in the residuals and remains below the threshold throughout the simulation, indicating a complete failure of spoofing detection. On the other hand, the residual statistics for the RAIM algorithm assisted by RDSS information gradually increase with the increase of the pull-off time, and once the alarm threshold is exceeded, it triggers an alert to the user that the system is being spoofed. Thus, it is evident that the RDSS-assisted method demonstrates superior spoofing detection performance compared to the RAIM algorithm that solely relies on RNSS information.

IV. Conclusions

This paper addresses the issue of vulnerability to spoofing interference in BDS RNSS positioning and timing services. Although traditional RAIM can detect and identify spoofing interference by detecting redundant observations, it fails when most or all satellites are spoofed. Methods based on external information assistance, such as IMU and high precision clocks, are expensive. In this paper, we propose a BDS spoofing detection and identification method using RDSS pseudo-range assistance to leverage the advantages of BDS RDSS being less susceptible to spoofing. The received RDSS pseudo-ranges of GEO satellites are involved in the least squares residuals algorithm to improve the spoofing detection capability. Simulation results demonstrate that the RDSS-assisted method effectively detects and identifies spoofed satellites even when most satellites or all satellites are spoofed, significantly improving the availability compared to traditional RAIM.

The utilization of RDSS pseudo-range observation as additional reference information for the RAIM algorithm enhances the spoofing detection and identification capability of the integrity algorithm, while capitalizing on the combined advantages of the high reliability of RDSS and the high precision of RNSS. Future research may focus on the fusion processing method of BDS RDSS and RNSS to improve the accuracy of deception interference detection, enhance PVT accuracy, and promote the widespread application of BDS in various industries.

References

[1] China Satellite Navigation Office. “BeiDou Navigation Satellite System Open Service Performance Standard (Version 3.0),” CSNO, Beijing, China, Tech. Rep. BDS-OS-PS-3.0, May. 2021.

[2] P. Risbud, N. Gatsis, and A. Taha, “Vulnerability analysis of smart grids to GPS spoofing. IEEE Transactions on Smart Grid,” IEEE Transactions on Smart Grid, vol. 10, no. 4, pp. 3535-3548, Jul. 2018.

[3] J. Li, H. Li, and M. Lu, (2020). “One‐dimensional traversal receiver autonomous integrity monitoring method based on maximum likelihood estimation for GNSS anti‐spoofing applications,” IET Radar, Sonar and Navigation, vol. 14, no. 2, pp. 1888-1896, Sep. 2020.

[4] Y. Gao, and G. Li, “A Slowly Varying Spoofing Algorithm Avoiding Tightly-Coupled GNSS/IMU With Multiple Anti-Spoofing Techniques,” IEEE Transactions on Vehicular Technology, vol. 71, no. 8, pp. 8864-8876, Aug. 2022.

[5] M. Spanghero, and P. Papadimitratos, “Detecting GNSS misbehaviour with high-precision clocks,” In Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks, Jun. 2021, pp. 389-391.

[6] F. Wang, C. Hu, S. Wu, Y. Tao, and Y. Xu. “Research on BeiDou anti-spoofing technology based on comprehensive radio determination satellite service,” Satellite Navigation, vol. 1, no. 1, pp. 1-9, Jan. 2020.

[7] Brown R G. Solution of the two‐failure GPS RAIM problem under worst‐case bias conditions: parity space approach[J]. Navigation, 1997, 44(4): 425-431.

[8] H. Kuusniemi, A. Wieser, G. Lachapelle and J. Takala, "User-level reliability monitoring in urban personal satellite-navigation," in IEEE Transactions on Aerospace and Electronic Systems, vol. 43, no. 4, pp. 1305-1318, October 2007, doi: 10.1109/TAES.2007.4441741.

[9] Angrisano A, Gioia C, Gaglione S, Del Core G (2013) GNSS reliability testing in signal-degraded scenario. Int J Navig Obs.Vol. 2013, Article ID 870365, 12 pages, 2013,doi:10.1115.