

Joint Spoofing and Multipath Suppression Using MEDLL and GNSS/5G/INS Consistency Check

Zihao Li¹, Yanhong Kou^{1*}, Xiaochen Guo¹ and Chundi Xiu¹

¹*School of Electronic Information Engineering, Beihang University, Beijing, China*

Abstract

Spoofing attacks and multipath interference, which are both highly correlated with authentic Global Navigation Satellite System (GNSS) signals, severely compromise reliable and accurate Positioning, Navigation, and Timing (PNT) services. Slowly varying spoofing gradually pulls the target receiver away from its true PNT state, while multipath introduces similar correlation peak distortions and code delay biases. Because these high-correlation interferences are difficult to separate and tend to coexist in real-world environments, this paper proposes a joint identification and suppression method based on the Multipath Estimating Delay Lock Loop (MEDLL) and a GNSS/5G/Inertial Navigation System (INS) observation consistency check. MEDLL first separates and estimates multiple signal components per satellite channel, from which the pseudorange residual consistency of each candidate component combination is constructed for preliminary grouping. Aided by 5G and INS references, spoofing and multipath components are reliably identified and suppressed, recovering normal navigation solutions for both standalone GNSS receivers and GNSS/5G/INS integrated systems. Experimental results on a public dataset demonstrate that under mixed slowly varying spoofing and multipath, the proposed method stably isolates authentic signals, achieving timing and positioning performance that approaches interference-free levels.

Keywords

GNSS/5G/INS tight coupling, slowly varying spoofing, multipath, consistency check, MEDLL

1. Introduction

Global Navigation Satellite System (GNSS)-based positioning, navigation, and timing (PNT) services serve as foundational infrastructure for civil aviation, intelligent transportation, power grid synchronization, mobile communications, and emergency rescue. However, weak signal power, publicly documented signal structures, and environmental reflections render GNSS highly susceptible to spoofing, multipath, and other radio-frequency interference [1, 2]. While antenna array and spatial filtering techniques are relatively mature for combating high-power jamming [3, 4], their ability to suppress spoofing and multipath signals arriving from directions near authentic signals is constrained, particularly on small-aperture, weight-constrained, or cost-sensitive platforms [5, 6].

Spoofing and multipath share the characteristic of being highly correlated with authentic signals in both time-frequency domain and waveform structure [7]. Slowly varying (or lift-off) spoofing gradually pulls the target user's position and timing estimates away from true values through subtle adjustment of code phase and carrier Doppler parameters. This slow variation closely resembles inherent Inertial Navigation System (INS) drift, causing conventional Kalman filter innovation-based abrupt-change detection to fail [8, 9, 10]. Multipath introduces similar correlation peak distortions and code delay biases, among which standing (quasi-static/resident) multipath, caused by fixed reflectors such as building walls and parked vehicles, is particularly difficult to eliminate through receiver tracking loop filtering or long-term averaging, in contrast to dynamic multipath [11, 12]. Both interference types manifest as multiple peaks, peak shift, asymmetry, and other deformations in the received signal's correlation function. More critically, their practical coexistence creates multiple highly correlated signal

WIPHAL'26: Work-in-Progress in Hardware and Software for Location Computation, Oct 06–08, 2026, Rome, Italy

*Corresponding author.

✉ zihao.li@buaa.edu.cn (Z. Li); kouy@buaa.edu.cn (Y. Kou); gxc327@buaa.edu.cn (X. Guo); xcd@buaa.edu.cn (C. Xiu)

🌐 <https://github.com/F612-f621/> (Z. Li); https://shi.buaa.edu.cn/kouyanhong/zh_CN/index.htm (Y. Kou)

🆔 0000-0002-9812-6677 (Y. Kou)



© 2026 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

components within a single satellite channel, making it hard to distinguish their individual contributions based solely on correlation peak shapes.

At the signal parameter estimation level, the Multipath Estimating Delay Lock Loop (MEDLL) based on the Maximum Likelihood (ML) criterion can estimate signal parameters of multiple components, but it inherently lacks the semantic capability to discern each component's origin (authentic, spoofing, or multipath) [13]. At the navigation information level of a tightly-coupled GNSS/INS integration, Extended Kalman Filter (EKF) innovation test can sense spoofing intrusion [9], but multipath interference similarly induces innovation anomalies, leading to high false alarm rates. Furthermore, under complete spoofing where all visible satellites are compromised, the spoofed signal set maintains internal GNSS consistency, making it impossible to distinguish the authentic set from the spoofed one using GNSS observations alone. External auxiliary information is therefore indispensable [14, 15].

Fifth-generation (5G) mobile communication signals, operating in frequency bands distinct from GNSS, provide independent Time of Arrival (TOA) and Angle of Arrival (AOA) measurements unaffected by GNSS spoofing, offering a reliable external reference [16, 17, 18, 19, 20]. To resolve the coexistence of slowly varying spoofing and multipath, this paper proposes a joint identification and suppression method based on MEDLL parameter estimation and a GNSS/5G/INS consistency check. Signal parameters extracted by MEDLL are grouped via pseudorange residual consistency, after which 5G/INS external references isolate authentic observations and reject interference so that normal navigation solutions at both standalone GNSS receiver and GNSS/5G/INS integrated system levels can be restored. Experimental results based on a publicly available dataset [20] show that the proposed method stably identifies authentic signal components under mixed spoofing and multipath interference, yielding recovered timing and positioning performance to near-interference-free levels.

2. MEDLL-based Parameter Estimation For Multiple High-Correlation Signals

Because spoofing, multipath, and authentic satellite signals share similar signal structures and high correlation, the MEDLL algorithm, originally designed for multipath estimation, can also be applied to extract spoofing parameters. The algorithm models the received GNSS (taking the BeiDou System, BDS, as a representative in the following) signal as a linear superposition of a finite number of signal components, estimating the amplitude $\hat{A}_i$, code delay $\hat{\tau}_i$, and carrier phase $\hat{\theta}_i$ of each component sequentially through iterative optimization [13, 20].

$$\begin{aligned}\hat{\tau}_i &= \arg \max_{\tau} \left\{ \text{Re} \left[\left(R_{\text{BDS}}(\hat{\tau}_i) - \sum_{k=0, k \neq i}^{\hat{M}} \hat{A}_k R_r(\hat{\tau}_i - \hat{\tau}_k) e^{j\hat{\theta}_k} \right) e^{-j\hat{\theta}_i} \right] \right\}, \\ \hat{A}_i &= \text{Re} \left[\left(R_{\text{BDS}}(\hat{\tau}_i) - \sum_{k=0, k \neq i}^{\hat{M}} \hat{A}_k R_r(\hat{\tau}_i - \hat{\tau}_k) e^{j\hat{\theta}_k} \right) e^{-j\hat{\theta}_i} \right], \\ \hat{\theta}_i &= \arg \left[R_{\text{BDS}}(\hat{\tau}_i) - \sum_{k=0, k \neq i}^{\hat{M}} \hat{A}_k R_r(\hat{\tau}_i - \hat{\tau}_k) e^{j\hat{\theta}_k} \right]\end{aligned}\quad (1)$$

In practice, MEDLL operates based on the input correlation function $R_{\text{BDS}}(\cdot)$ and a locally generated reference correlation function $R_r(\cdot)$. The specific steps include: (1) Preprocessing: generate the reference correlation function $R_r(\tau)$ for each satellite using clean, interference-free signals; (2) Iterative estimation: estimate the parameters of the first signal component using the ML criterion and reconstruct its correlation function based on the reference; (3) Residual update: subtract the reconstructed correlation from the input correlation $R_{\text{BDS}}(\tau)$ and use the residual to estimate the next component; (4) Loop convergence: repeat the above process until all components are estimated or the residual energy falls below a preset threshold. Iteration also terminates if the change in the estimated code delay between two successive iterations is less than the sampling interval. To accommodate coexist-

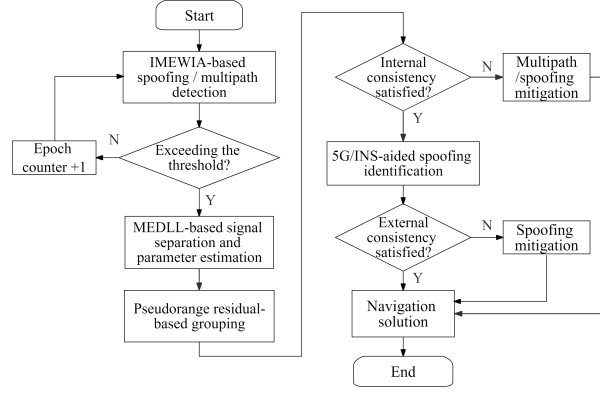


Figure 1: Anti-spoofing and anti-multipath procedure based on BDS/5G/INS consistency check

ing spoofing and multipath, the maximum number of estimated components per channel, $\hat{M}$, is set to 3, enabling simultaneous processing of the direct signal, a spoofing signal, and the most energetic multipath component.

After MEDLL has estimated two or three code delays $\hat{\tau}_i^k$ ($i = 1, 2, 3$) for the k -th satellite, pseudorange candidates $\hat{\rho}_i^k$ are recovered based on the initial pseudorange $\hat{\rho}_0^k$ corresponding to the code phase $\hat{\tau}_0^k$ of the input correlation tracked by the receiver's delay lock loop:

$$\hat{\rho}_i^k = \hat{\rho}_0^k + c \left(\hat{\tau}_i^k - \hat{\tau}_0^k \right) \quad (2)$$

where c is the speed of light. Thus, MEDLL accomplishes signal separation and parameter estimation, providing two or three independent pseudorange measurements for each affected satellite to feed the subsequent consistency check.

3. Mixed Spoofing-Multipath Identification and Suppression Based on GNSS/5G/INS Consistency Check

After MEDLL completes separation and pseudorange estimation, two or three candidate pseudoranges are available per satellite channel. However, MEDLL itself cannot determine which component corresponds to the authentic satellite, spoofing, or multipath. This section establishes a complete processing framework using the pseudorange residual statistic as the primary feature for grouping, identification, and interference mitigation.

3.1. Anti-Spoofing and Anti-Multipath Procedure Based on Consistency Check

At the GNSS information level, when five or more pseudorange equations are available, the solution process becomes an overdetermined adjustment problem, and the residuals reflect the degree of consistency among the signal components: authentic satellite signals are necessarily mutually consistent, signals from a single spoofing source are also mutually consistent, authentic and spoofed signals conflict, and multipath components lack consistency across channels and with authentic or spoofing signals due to random reflection paths. Based on these facts, the pseudorange residual is adopted as the core feature for consistency check. Fig. 1 illustrates the overall anti-spoofing and anti-multipath procedure.

The Improved Multi-Epoch Weighted Innovation Accumulation (IMEWIA) detector proposed in [18] constructs detection statistics by accumulating EKF innovations over a sliding window. It can detect both slowly varying spoofing-induced innovation offsets and multipath-induced anomalies. Once an alarm is triggered, MEDLL is activated to estimate the parameters of each signal component of affected satellite channels and recover multiple pseudorange sets. The consistency check stage then begins: first, the combination with the best internal consistency is selected as the reference group

via exhaustive permutation; then, remaining components are sequentially tested for consistency with the reference group. Finally, aided by 5G and INS measurements, each group is labeled as authentic, spoofing, or multipath, and anomalous components are eliminated/excluded at both the standalone BDS receiver level and the BDS/5G/INS tightly-coupled system level, restoring the normal navigation solution.

The procedure accommodates three interference scenarios—spoofing only, multipath only, and co-existing spoofing and multipath—each following a distinct processing flow.

3.2. Pseudorange Residual Statistic

The pseudorange residual reflects self-consistency among a set of measurements: if all components originate from the same spatial-temporal reference (e.g., all from authentic satellites or all from a single spoofer), the residual should be lower than the preset threshold; otherwise, it increases significantly [14].

For a combination Ω_K^j , $j = 1, 2, \dots, 3^K$, selecting one candidate pseudorange from each of K channels ($5 \leq K \leq N_s$, where N_s is the total number of tracked satellites), the measurement equation is

$$\rho_{(\Omega_K^j)}^k = \|\mathbf{p}^k - \mathbf{p}_u\| + c \cdot \delta t_u + \varepsilon^k \quad (3)$$

where $\mathbf{p}^k$ is the satellite position, $\mathbf{p}_u$ and δt_u are the unknown user position and clock bias, and $\varepsilon^k \sim \mathcal{N}(0, \sigma_k^2)$, with σ_k^2 from the EKF measurement noise covariance. Weighted least squares with the weight matrix $W = \text{diag}(1/\sigma_k^2)$ yields the estimated position $\hat{\mathbf{p}}_u$ and clock bias $\hat{\delta t}_u$, giving predicted pseudorange

$$\hat{\rho}_{(\Omega_K^j)}^k = \|\mathbf{p}^k - \hat{\mathbf{p}}_u\| + c \cdot \hat{\delta t}_u. \quad (4)$$

The pseudorange residual is the difference between the actually-measured and the predicted pseudoranges, and the weighted sum-of-squares statistic for the combination is

$$S(\Omega_K^j) = \sum_{k=1}^K \left(\frac{\rho_{(\Omega_K^j)}^k - \hat{\rho}_{(\Omega_K^j)}^k}{\sigma_k} \right)^2 \sim \chi^2(K-4), \quad (5)$$

which follows a central chi-square distribution when all components share the same spatial reference and a non-central chi-square distribution when components from different references are mixed. Multiple epochs can be accumulated to enhance reliability. In practice, five satellites are randomly chosen; the combination with minimum S below the threshold $T_\rho = F_S^{-1}(1 - P_{fa} \mid K-4)$ (when P_{fa} is the preset false-alarm rate) becomes the reference set. Remaining channels are added sequentially, and all components are grouped according to whether the joint residual falls below the threshold.

3.3. Authentic, Spoofing, and Multipath Group Identification Aided by 5G/INS

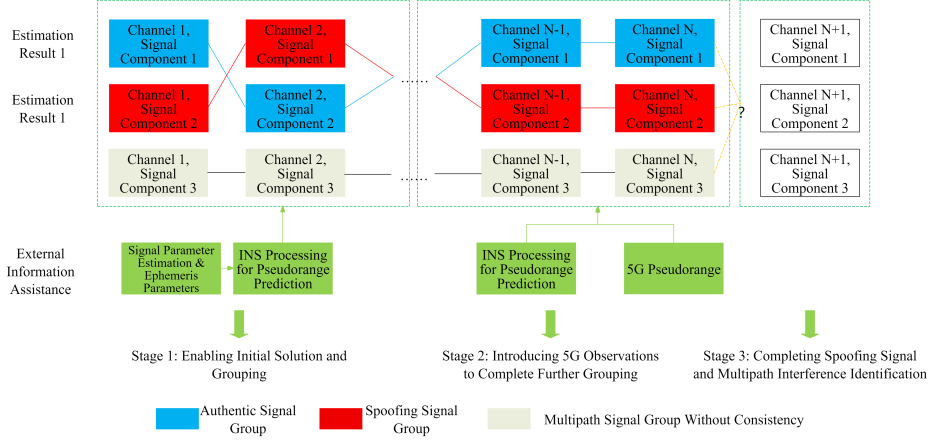
Under complete spoofing, the above grouping yields two internally consistent sets, but their true identities cannot be determined from internal consistency alone. 5G and INS serve as external spatial references. For each group under test, the BDS pseudoranges are jointly processed with all the 5G pseudoranges $\{\rho_{5G}^m\}_{m=1}^{N_g}$ from N_g Base Stations (BSs) via a combined least-squares adjustment that estimates the common user position and clock bias, yielding the joint residual statistic

$$S_{\text{Grp}+5G}(\Omega_K^j) = \sum_{k=1}^K \left(\frac{\rho_{(\Omega_K^j)}^k - \hat{\rho}_{(\Omega_K^j)}^k}{\sigma_k} \right)^2 + \sum_{m=1}^{N_g} \left(\frac{\rho_{5G}^m - \hat{\rho}_{5G,(\Omega_K^j)}^m}{\sigma_{5G}^m} \right)^2 \sim \chi^2(K + N_g - 4), \quad (6)$$

Table 1

Identification criteria before and after combination with 5G/INS

Component Property	Without 5G/INS	With 5G/INS
Authentic signal group	$S_{\text{au}} < T_\rho$	$S_{\text{au}+5G/INS} < T_\rho$
Spoofing signal group	$S_{\text{sp}} < T_\rho$	$S_{\text{sp}+5G/INS} > T_\rho$
Multipath signal group	$S_{\text{mp}} > T_\rho$	$S_{\text{mp}+5G/INS} > T_\rho$

**Figure 2:** Authentic, spoofing, and multipath signal component group identification process based on BDS/5G/INS integration

where $\hat{\rho}_{5G,(\Omega_K^j)}^m$ is the predicted pseudorange from the joint adjustment using the K BDS pseudoranges of the candidate group and all the N_g 5G pseudoranges, and σ_{5G}^m is the 5G measurement noise standard deviation.

Alternatively, when available 5G BSs are insufficient, the INS short-term position $\mathbf{P}_{\text{INS}}$ can be incorporated as an a priori constraint. With an assumed position uncertainty σ_{INS} , this adds a penalty term $\|\hat{\mathbf{P}}_u - \mathbf{P}_{\text{INS}}\|^2 / \sigma_{\text{INS}}^2$ to the least-squares objective, resulting in the joint statistic

$$S_{\text{Grp}+\text{INS}}(\Omega_K^j) = \sum_{k=1}^K \left(\frac{\rho_{(\Omega_K^j)}^k - \hat{\rho}_{(\Omega_K^j)}^k}{\sigma_k} \right)^2 + \frac{\|\hat{\mathbf{P}}_u - \mathbf{P}_{\text{INS}}\|^2}{\sigma_{\text{INS}}^2} \sim \chi^2(K-4). \quad (7)$$

The identification criteria before and after combining with the 5G/INS reference are summarized in Table 1.

With BDS alone, both authentic and spoofing groups yield residuals below the threshold and cannot be distinguished. Once the 5G/INS external reference is introduced, the authentic group retains consistency while the spoofing group's residual rises. Components inconsistent with either of the above groups are multipath. Fig. 2 illustrates this sequential identification process.

While exhaustive permutation-based grouping introduces exponential complexity with increasing satellites and multipath components, this data association problem can be scaled in future work using rigorous Bayesian frameworks [21].

3.4. High-Correlation Interference Suppression and Navigation Solution Recovery

Upon component identification, high-correlation anomaly suppression occurs at two levels. At the standalone BDS receiver level, spoofing/multipath are cancelled via correlation-domain reconstruction, or only the identified authentic measurements are selected for PVT computation. At the BDS/5G/INS integrated system level, confirmed authentic BDS measurements, 5G pseudorange/AOA and INS predictions are fused. The tightly-coupled EKF exploits multi-source sensor redundancy to improve posi-

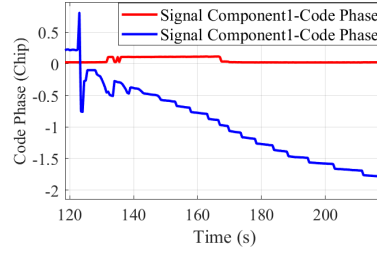


Figure 3: MEDLL code phase estimation for PRN 7 before and after spoofing

tioning accuracy and continuity with spoofed/multipath components excluded, providing robust performance even when some satellite channel components cannot be fully recovered.

4. Simulation Experiments and Result Analysis

The publicly available BDS/5G/INS dataset [20] contains seven scenarios with diverse vehicle maneuvers, multipath conditions, and reasonably designed spoofing parameters, each providing BDS B1I intermediate frequency signals, 5G TOA/AOA measurements, and INS data at three grades (consumer, tactical, and navigation). The results of Scenario 4 are selected to be presented here. This scenario employs a tactical-grade Inertial Measurement Unit (IMU) and subjects all ten visible satellites to a 1.5-chip common-mode time spoofing pull-off during 120–190 s, followed by a non-common-mode position spoofing with a 60 m eastward shift during 190–220 s. The spoofing-only case is examined; standing multipath is then added to four low-elevation satellites over [85, 120) s and [150, 170) s to evaluate performance under coexisting spoofing and multipath.

4.1. Scenario with Spoofing Only

Taking the PRN 7 satellite as an example, Fig. 3 shows code phase estimation results for two signal components separated by MEDLL after spoofing intrusion. Two sets of candidate pseudoranges are recovered for subsequent grouping.

Fig. 4 shows the BDS pseudorange combination reference determination process (left) and the authentic/spoofing group identification process aided by 5G observations from one or two BSs (right). First, the combination with minimum pseudorange residual among MEDLL components of five satellites is selected as reference. Among 17 permutations, only the “AAAAA” and “BBBBB” combinations satisfy consistency criteria. Based on this, the remaining satellite signal components are sequentially grouped. As shown in the right part of Fig. 4, when adding each satellite, one of the two combinations maintains a residual below the threshold while the other rises rapidly, naturally forming two groups, A and B. Finally, when combined with 5G/INS references, Group B maintains a significantly smaller residual than Group A. Therefore, Group B is confirmed as authentic and Group A as spoofing.

Fig. 5 presents the Geometric Dilution of Precision (GDOP) for 10 BDS satellites before and after integrating 5G observations from one or two BSs. Integrating 5G measurements evidently reduces GDOP across all epochs compared to BDS alone. Despite GDOP fluctuations caused by 5G BS handovers as the vehicle moves, its overall value stays lower than the BDS-only case, reflecting improved positioning geometry contributed by 5G anchors.

Fig. 6 shows standalone BDS (solid lines) and BDS/5G/INS integrated (dotted lines) navigation solutions before and after spoofing suppression. Without suppression, the time spoofing during [120, 190) s drives the timing error from near zero to 219.8 m (corresponding to the 1.5-chip common-mode pull-off of the B1I signal). After suppression, a brief transient jitter caused by limited sampling rate and MEDLL resolution is observed, but the timing and positioning errors quickly stabilize around zero. The subsequent position spoofing during [190, 220) s disrupts both the timing and eastward positioning solutions; following suppression, both errors return to near zero, close to the pre-spoofing levels.

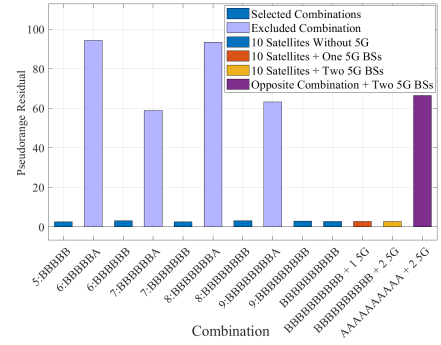
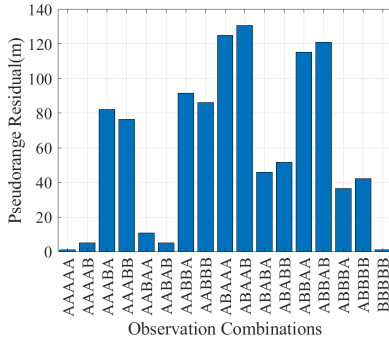


Figure 4: BDS pseudorange combination reference determination (left) and authentic/spoofing group identification aided by one/two 5G BSs (right)

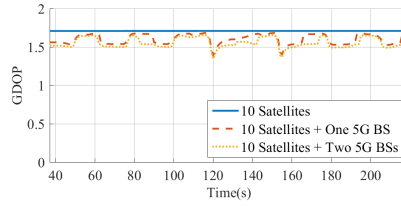


Figure 5: GDOP values before and after BDS and 5G integration

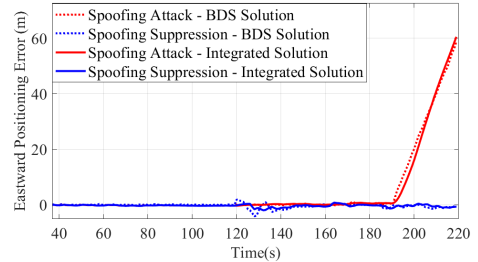
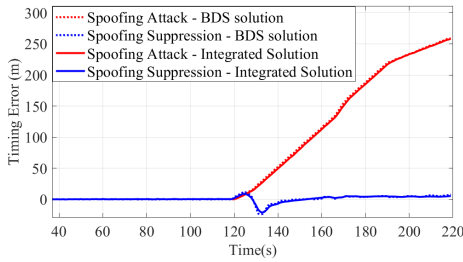


Figure 6: Standalone BDS and BDS/5G/INS integrated solutions before and after spoofing suppression: timing error (left) and eastward positioning error (right)

Throughout the test, the integrated solution consistently outperforms the standalone BDS solution.

4.2. Scenario with Coexisting Spoofing and Multipath Interference

During the [150, 170] s interval, the system suffers from concurrent spoofing attacks and multipath interference. Fig. 7 illustrates signal component grouping and identification process at $t = 160$ s. First, the reference is selected from the combination of five BDS satellites with the minimum pseudorange residual. Then, signal components of the remaining satellites are added one by one and screened via pseudorange consistency until all 10 tracked visible satellite channels are included. With the aid of INS measurements, the first and second groups are identified as authentic and spoofing components, respectively, whereas the remainder as multipath components.

Similar to Section 4.1, Fig. 8 shows the timing error (left) and 3D positioning errors (right) before and after joint spoofing and multipath suppression. For the standalone BDS solution, without interference suppression, the timing error and 3D positioning error rise to 136.16 m and 166.32 m, respectively. After joint suppression and recovery, both return to near zero with Root Mean Square Error (RMSE) values of 4.37 m and 6.76 m. For the BDS/5G/INS integrated solution, without suppression, the timing error and 3D positioning error reach 78.00 m and 92.87 m at the 220th second. After suppression and recovery, both return to near zero with RMSEs of 4.29 m and 3.38 m. These results indicate that under the proposed procedure, the system can achieve effective interference suppression and stable navigation solution recovery even when spoofing and multipath coexist with different code pull-off

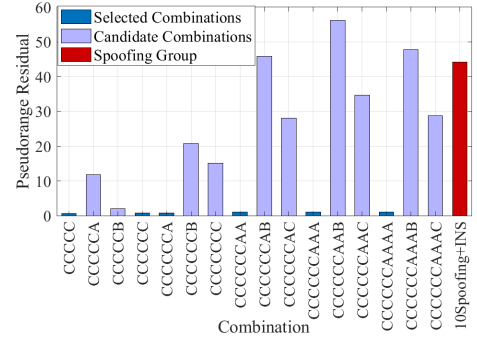
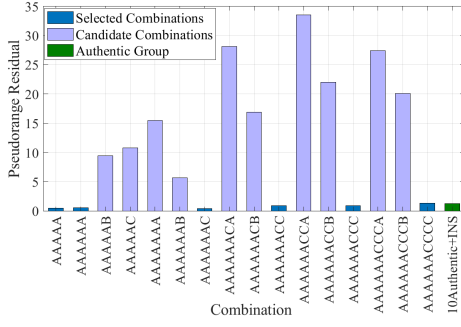


Figure 7: INS-aided BDS authentic signal component group (left) and spoofing/multipath component group (right) identification process at the 160th second under coexisting spoofing and multipath

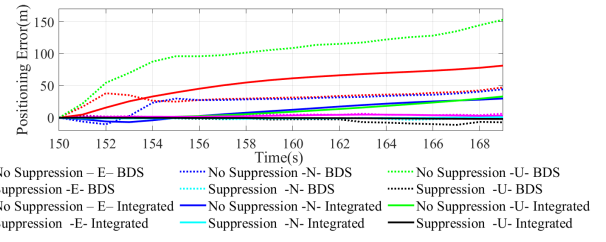
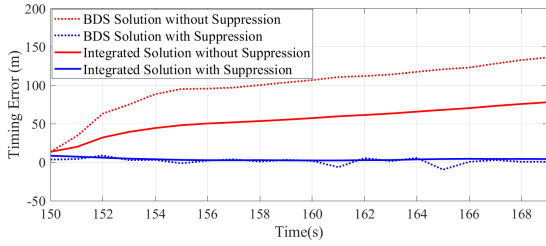


Figure 8: Standalone BDS and BDS/5G/INS integrated solutions before and after joint spoofing and multipath suppression: timing error (left) and east/north/up positioning errors (right)

rates. Compared with the interference free RMSE of 0.52 m reported in [20], the degradation primarily stems from the limited estimation accuracy of MEDLL, which is constrained by the sampling rate and code phase resolution, particularly under short delay multipath conditions.

For brevity, only Scenario 4 is presented in detail; however, the proposed method has been verified across all seven dataset scenarios. It should be noted that in practical urban canyon deployments, 5G signals are susceptible to Non-Line-of-Sight (NLoS) propagation as well as to synchronization errors both among BSs and between the BS and the user, which may introduce significant biases into TOA/AOA measurements, thereby potentially degrading the performance of the proposed method. In addition, while the simulation focused on standing multipath as the representative challenging case, the underlying consistency check logic is in principle not restricted to this multipath type and can be extended to dynamic multipath environments.

5. Conclusion

This paper proposed a joint identification and suppression method based on MEDLL parameter estimation and GNSS/5G/INS observation consistency check to address the challenge of coexisting slowly varying spoofing and multipath. MEDLL separates and estimates multi-component signal parameters per satellite channel, pseudorange residuals construct the consistency statistic to group components, and 5G/INS auxiliary information isolates authentic components from spoofing and multipath so that interference can be jointly suppressed at both standalone GNSS and GNSS/5G/INS integrated navigation levels. Experimental results demonstrate that the proposed method effectively separates and identifies signal component origins, and the recovered clock bias and 3D positioning RMSEs approach the interference-free level, validating the method's effectiveness under mixed high-correlation interference. Future work will extend the framework to more challenging scenarios, incorporate Bayesian data association to improve scalability, and evaluate robustness under dynamic multipath, 5G NLoS propagation, and unsynchronized BS conditions.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (Grant No. U24B6013).

Declaration on Generative AI

During the preparation of this work, the authors used DeepSeek in order to: Grammar and spelling check. After using this service, the authors reviewed and edited the content as needed and take full responsibility for the publication's content.

References

- [1] D. Schmidt, K. Radke, S. Camtepe, E. Foo, and M. Ren, "A survey and analysis of the GNSS spoofing threat and countermeasures," *ACM Comput. Surv.*, vol. 48, pp. 1–31, 2016.
- [2] M. L. Psiaki and T. E. Humphreys, "GNSS spoofing and detection," *Proc. IEEE*, vol. 104, pp. 1258–1270, 2016.
- [3] M. D. Zoltowski and A. S. Gecan, "Advanced adaptive null steering concepts for GPS," in *Proc. IEEE MILCOM*, 1995, pp. 1214–1218.
- [4] S. Daneshmand, A. J. Jahromi, A. Broumandan, and G. Lachapelle, "GNSS space-time interference mitigation and attitude determination in the presence of interference signals," *Sensors*, vol. 15, pp. 12180–12204, 2015.
- [5] S. B. Lee, S. H. Seo, and G. I. Jee, "Performance assessment of real-time GNSS spoofing detection with IMU measurements on Android smartphones," in *Proc. ION GNSS+*, 2024, pp. 2520–2530.
- [6] M. Ceccato, F. Formaggio, G. Caparra, N. Laurenti, and S. Tomasin, "Consumer INS coupled with carrier phase measurements for GNSS spoofing detection," *arXiv preprint, arXiv:2502.03619*, 2025.
- [7] L. Meng, L. Yang, W. Yang, and L. Zhang, "A survey of GNSS spoofing and anti-spoofing technology," *Remote Sens.*, vol. 14, no. 19, p. 4826, 2022.
- [8] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner Jr., "Assessing the spoofing threat: Development of a portable GPS civilian spoofer," in *Proc. ION GNSS*, 2008, pp. 2314–2325.
- [9] X. Jin, X. Zhang, S. Li, and S. Zheng, "Detection of slowly varying spoofing using weighted Kalman gain in GNSS/INS tightly coupled systems," *GPS Solut.*, vol. 28, no. 1, p. 54, 2024.
- [10] Y. Gao and G. Li, "A slowly varying spoofing algorithm avoiding tightly coupled GNSS/IMU with multiple anti-spoofing techniques," *IEEE Trans. Veh. Technol.*, vol. 71, no. 8, pp. 8864–8876, 2022.
- [11] A. J. Van Dierendonck, P. Fenton, and T. Ford, "Theory and performance of narrow correlator spacing in a GPS receiver," *Navigation*, vol. 39, no. 3, pp. 265–283, 1992.
- [12] P. D. Groves, Z. Jiang, M. Rudi, and P. Strode, "A portfolio approach to NLOS and multipath mitigation in dense urban areas," in *Proc. ION GNSS+*, 2013, pp. 3231–3247.
- [13] Y. Wang, Y. Kou, Z. Huang, and Y. Zhao, "GNSS spoofing maximum-likelihood estimation switching between MEDLL and CADLL," *GPS Solut.*, vol. 27, no. 3, p. 148, 2023.
- [14] Y. Wang, Y. Kou, Z. Huang, "GNSS spoofing identification with assistance of LEO satellite signal," in *Proc. ION ITM*, 2023, pp. 708–724.
- [15] Y. Liu, S. Li, Q. Fu, and Z. Liu, "Analysis of Kalman filter innovation-based GNSS spoofing detection method for INS/GNSS integrated navigation system," *IEEE Sensors J.*, vol. 19, no. 13, pp. 5167–5178, 2019.
- [16] L. Bai, C. Sun, A. G. Dempster, H. Zhang, and W. Feng, "GNSS spoofing detection and mitigation with a single 5G base station aiding," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 60, no. 4, pp. 4601–4620, 2024.
- [17] J. Liu, K. Gao, W. Guo, J. Cui, and C. Guo, "Role, path, and vision of '5G+ BDS/GNSS'," *Satell. Navig.*, vol. 1, no. 1, p. 23, 2020.
- [18] Z. Li and Y. Kou, "Lift-off Spoofing Detection for GNSS/5G/INS Tightly-Coupled Systems," in *Proc. ICGNC*, 2026, accepted.
- [19] W. Guo, C. Ji, S. Qi, Q. Zhang, X. Meng, and W. Song, "Preliminary performance analysis of tightly-coupled 5G/PPP positioning based on different 5G observations," *IEEE Trans. Instrum. Meas.*, vol. 74, pp. 1–13, 2025.
- [20] Z. Li and Y. Kou, "Dataset constructions for anti-spoofing testing in BDS/5G/INS integrated navigation," in *Proc. IEEE UPINLBS*, 2025.
- [21] F. Meyer, T. Kropfreiter, J. L. Williams, et al., "Message Passing Algorithms for Scalable Multitarget Tracking," in *Proc. of the IEEE*, vol. 106, no. 2, pp. 221–259, Feb. 2018.