Received: 12 June 2025 | Revised: 16 March 2026 | Accepted: 12 July 2026

DOI: 10.33012/navi.789

ORIGINAL ARTICLE

A GNSS/IMU Spoofing Detection Method Based on Motion Models for Vehicular Navigation

Yimin Ma | **Mingquan Lu** | **Hong Li***

[1] Department of Electronic Engineering, Tsinghua University, State Key Laboratory of Space Network and Communications, Beijing National Research Center for Information Science and Technology, Beijing, 100084, China

Correspondence
Hong Li
Email: lihongee@tsinghua.edu.cn

Abstract

Given the wide application of inertial measurement units (IMUs) in vehicular navigation, IMU-aided global navigation satellite system (GNSS) spoofing detection methods have gained significant attention. One of the most effective detection methods utilizes IMU and GNSS measurements to achieve velocity increment direct comparison (VIDC). However, this intuitive approach shows unsatisfactory performance when facing concealed spoofing deviations and low-cost vehicle-mounted IMUs. To address this issue, we propose a motion-model-based (MM-based) VIDC spoofing detection method by exploiting vehicular kinematic characteristics to enhance the detection performance. The proposed method utilizes motion models to impose physically interpretable and low-dimensional constraints on velocity increment deviations, decreasing the uncertainty in detection. This paper elaborates on the principle of this method, derives the theoretical performance of different-order MM-based methods, and describes the relationship between orders of the optimal detection model and spoofing deviation. Simulations and field experiments demonstrate that the MM-based method achieves an approximately 30% higher detection rate than the conventional approach.

Keywords

GNSS, IMU, motion model, spoofing detection, vehicular navigation, velocity increment

1 | INTRODUCTION

Resilient position, velocity, and timing (PVT) information is the cornerstone for a broad range of vehicular navigation applications, including route planning, autonomous driving, intelligent transportation, and unmanned delivery (Joubert et al., 2020). Global navigation satellite systems (GNSSs) are acknowledged as a pivotal component of vehicular navigation systems, providing continuous, convenient, and accurate PVT information (Kaplan & Hegarty, 2017). Nevertheless, GNSSs are susceptible to spoofing attacks, which can manipulate users into acquiring erroneous PVT outcomes without being detected (Mina et al., 2024). With the rapid development of spoofing devices and strategies, GNSS spoofing incidents have become increasingly frequent and have occurred globally, posing significant threats to the security of vehicular navigation. In addition, as the international standard for

Licensed under CC-BY 4.0 © 2026 Institute of Navigation

automotive cybersecurity, i.e., ISO/SAE 21434 (Schmittner et al., 2018), continues to be promoted, which encompasses scenarios involving GNSS spoofing, there is a growing focus on enhancing the spoofing defense capabilities of vehicles.

Multiple effective approaches have been proposed for detecting GNSS spoofing attacks (Meng et al., 2022). From the perspective of the GNSS receiver processing chain, existing approaches can be generally categorized into three levels: signal-level methods, raw-measurement-level methods, and navigation-solution-level methods. Signal-level approaches typically operate in the acquisition and tracking stages. Representative techniques include signal authentication such as open service navigation message authentication (OSNMA) for Galileo and chips message robust authentication (Chimera) for the Global Positioning System (GPS) (Humphreys, 2013; Mina et al., 2022; Motella et al., 2021), as well as multi-acquisition peak detection (Li et al., 2020), signal quality monitoring methods (C. Sun et al., 2018; Zhang et al., 2024), and other related techniques (Wu et al., 2020). Raw-measurement-level methods utilize GNSS observables, including pseudorange, carrier phase, and Doppler frequency, to detect inconsistencies caused by spoofing, such as receiver autonomous integrity monitoring (Parkinson & Axelrad, 1988; L. Wang et al., 2025), Doppler residual monitoring (Z. Wang et al., 2021), and others (Psiaki et al., 2014; H. Wang et al., 2024). The third category operates at the navigation-solution level and includes approaches such as clock monitoring (Shang et al., 2020), sensor-aided consistency checking (Chang et al., 2022; Dasgupta et al., 2022), and so on (Zhou et al., 2023). It is noted that each category has distinct characteristics and applicable scenarios. In practice, GNSS spoofing defense is typically implemented as a multi-layer protection framework, and the specific defense strategy utilized should depend on the system architecture and available information.

Considering that most vehicular navigation systems employ commercial GNSS receivers and are commonly equipped with multiple onboard sensors (Cao et al., 2022; Zhuang et al., 2023), sensor-aided spoofing detection has attracted increasing attention. These approaches directly cross-check the physically independent and resilient PVT information provided by sensors against potentially compromised GNSS navigation solutions, thereby reducing the reliance of spoofing detection on prior assumptions about the spoofing source (L. Wang et al., 2024). Furthermore, as a navigation-solution-level defense strategy, the use of external sensors complements rather than competes with other spoofing detection techniques, serving as a second-layer safeguard within an integrated navigation architecture. For vehicular navigation in particular, navigation systems that integrate GNSS and inertial measurement unit (IMU) data have become one of the most widely adopted and commercially mature frameworks (Gao et al., 2021; He et al., 2023). Consequently, enhancing spoofing resilience within GNSS/IMU systems can significantly improve the security of a large proportion of current vehicle navigation systems.

Existing IMU-aided spoofing detection methods can be divided into fusion abnormality detection (FAD) and independent consistency monitoring (ICM) methods (Ma et al., 2024). FAD techniques involve utilizing intermediate variables of specific fusion systems for spoofing detection, including innovation-based methods (Liu et al., 2019; Tanıl et al., 2018), residual-based methods (Crespillo et al., 2017; Khanafseh et al., 2014; Kujur et al., 2024), and state-based methods (Chang, Zhang, et al., 2023; Jiang et al., 2019; Xu et al., 2018). These methods can benefit from the accurate estimation of sensor parameters provided by fusion systems. However, as distinct GNSS/IMU fusion frameworks continue to emerge, most effective FAD algorithms, which were originally designed for extended Kalman filter (EKF) systems, face great challenges in being directly applied to new frameworks

such as optimization-based or learning-based systems (Zhuang et al., 2023). In contrast, ICM methods are independent of fusion frameworks and detect spoofing by directly verifying the consistency of information provided by GNSS and IMU measurements (Curran & Broumendan, 2017; Kwon & Shim, 2020; Lee et al., 2015; Lo et al., 2017; Wei et al., 2022). ICM techniques operate prior to data fusion; thus, they can be modular, system-independent, and easy to implement across various fusion system architectures. These methods also serve as first-line spoofing defense strategies before FAD techniques and are thus crucial for enhancing spoofing resilience in vehicular navigation.

Many IMU-aided ICM algorithms have been proposed thus far, and their basic principle lies in comparing velocity increments measured by GNSS and IMU, which are equivalent to average accelerations for constant intervals. One well-known method is denoted here as the velocity increment direct comparison (VIDC) method, in which the difference between two velocity increments or accelerations is directly monitored (Narain et al., 2019). The initial idea of VIDC was proposed by Lee et al. (2015): the detector raises an alarm when the difference exceeds a preset threshold due to velocity increment deviation induced by spoofing, whereas the difference should be close to zero under spoofing-free scenarios. The study of Lo et al. (2017) clarified the implementation steps and presented field experimental verification utilizing aerial data. Kwon and Shim (2020) provided a detailed theoretical derivation for the detector and evaluated the performance of distinct directions as decision variables. In addition, the Pearson correlation and wavelet coherence were utilized by Curran and Broumendan (2017) and Neish et al. (2018) to conduct vehicular experiments based on consistency checking between GNSS and IMU data. However, the performance of these methods typically relies on a long detection window and rapid motion fluctuations. A spoofing detection rate of approximately 0.6 can be achieved with a time-to-alarm of up to 120 s with a false-alarm probability of 0.001. In addition, Ceccato et al. (2021) proposed a generalized likelihood ratio test (GLRT)-based detector with reported performance gains; however, this detector requires an additional magnetometer and exhibits a computational complexity 2–3 orders higher than that of previous methods. Wei et al. (2022) proposed a defense method that exploits estimation residuals of the coordinate transformation matrix during the initial startup phase. However, this method requires long-duration pre-integration of IMU measurements, which can introduce substantial accumulated errors.

In summary, most existing approaches assess only the numerical consistency between GNSS and IMU measurements, without incorporating the underlying physical characteristics and constraints related to sensors and carriers. This single-dimensional consistency check limits the detection performance of these methods in vehicular navigation. It has been verified that the detection rate of the conventional VIDC method reaches only approximately 30% with a low-accuracy IMU, with an average spoofing deviation of 0.3 m/s under common scenarios when the false-alarm rate is set to 0.01 (Ma et al., 2025). This limitation originates from smaller spoofing deviations and higher noise levels. Specifically, increasingly sophisticated spoofing strategies targeting vehicles can introduce subtle deviations that evade detection (Chang, Huang, et al., 2023; Geng et al., 2024). Additionally, to reduce production costs, vehicles commonly rely on low-cost micro-electromechanical system IMUs with limited accuracy (Sasani et al., 2016; Y. Sun et al., 2022), which further increases the noise level in measurements.

To enhance detection performance, this paper focuses on fully involving vehicular motion characteristics in detection by introducing motion models to impose physically interpretable constraints on velocity increment deviations in GNSS and

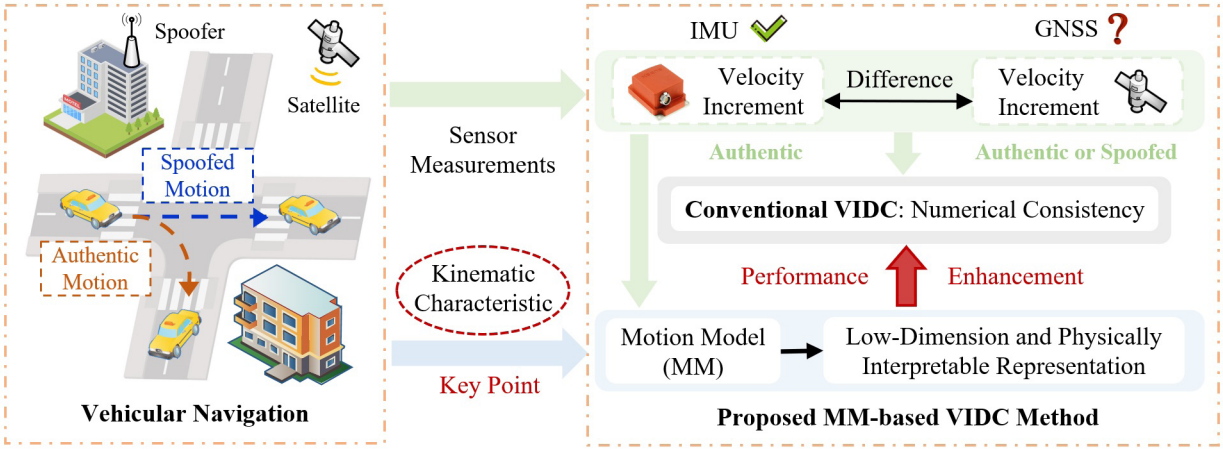


FIGURE 1 Basic framework of the proposed MM-based VIDC spoofing detection method for IMU-equipped vehicles

IMU measurements. As illustrated in Figure 1, this approach transforms the conventional VIDC problem of directly monitoring the velocity increment difference into a process of model matching and detecting. The accurate, low-dimensional parameterized representation based on a motion model can reduce the uncertainty of spoofing deviation, thereby reducing the degrees of freedom in detection and improving performance.

The rationality of our core idea stems from the fact that the velocity increment deviation essentially reflects the discrepancy between IMU-measured authentic motion and GNSS-measured motion, which is vulnerable to spoofing. Within a short detection window, both the authentic vehicular motion and the spurious state forged by a spoofer specifically designed for vehicles can be approximated by motion models; for example, uniform-velocity or uniform-acceleration driving can be represented by a first-order polynomial velocity model (Broumandan & Lachapelle, 2018). Even for other commonly spurious motions such as circular trajectories, motion models remain valid over brief intervals, allowing the velocity increment deviation to be accurately represented.

Thus, this paper proposes a motion model-based (MM-based) VIDC technique for IMU-equipped vehicles to enhance the performance of GNSS spoofing detection. By incorporating vehicular kinematic characteristics, the proposed approach imposes physically meaningful constraints on spoofing-induced deviations. Detection statistics are derived, and the theoretical performance of MM-based detectors under various spoofing scenarios is analyzed. Simulations explore the influencing factors of the MM-based method and assess its quantitative detection performance. In addition, vehicular field experiments are conducted to validate the effectiveness of the proposed method and to analyze the impact of equivalent driving time on motion order. The main contributions of this work can be summarized as the following three aspects:

1) Motion Model: Motion models are innovatively applied to GNSS/IMU spoofing detection in our MM-based VIDC method, introducing vehicular kinematic constraints that provide physically grounded restrictions and effectively reduce detection uncertainty compared with the conventional VIDC method. As a form of ICM technique, the proposed MM-based method also offers many advantages, most notably its applicability to all types of GNSS/IMU fusion systems.

2) Performance Analysis: A theoretical framework is established to reveal how the performance of MM-based VIDC detectors depends on the order of spoofing deviations. The analysis clarifies the balance between dimension gain and model loss and identifies the conditions under which different model orders offer optimal performance.
3) Practical Evaluation: Vehicular field experiments are carried out to validate the proposed detection framework. The results explore the performance of distinct-order MM-based VIDC methods and confirm significant performance improvements over the conventional approach, demonstrating an enhancement of approximately 30%.

The remainder of this paper is organized as follows. Section 2 describes the measurement model and reviews the conventional VIDC method. Section 3 illustrates the basic principle of the MM-based VIDC method and derives its detection statistics. A theoretical performance comparison and influencing factor analysis are presented in Section 4, based on derivation and simulations. Section 5 presents field vehicular experiment results, and the paper is concluded in Section 6.

2 | MEASUREMENT MODEL AND CONVENTIONAL VIDC METHOD

This section firstly describes velocity increment measurements obtained by an IMU and GNSS independently. Then, the basic principle of the conventional VIDC method is reviewed for a subsequent performance comparison.

2.1 | Velocity Increments Measured by IMU and GNSS

The raw measurements of an IMU include acceleration measured by an accelerator and angular velocity measured by a gyroscope, which are initially expressed in the body frame (b-frame) of the IMU with x, y, and z directions. The position and velocity are GNSS measurements expressed in the navigation system (n-frame), which is usually chosen as the north–east–down frame with N, E, and D directions. The spatial relationship between these two frames can be represented by a coordinate transformation matrix.

The IMU obtains velocity increments via pre-integration (Wei et al., 2020). Denoting raw IMU measurements of acceleration and angular velocity at epoch k as $\tilde{\mathbf{a}}_{\mathrm{I},k}$ and $\tilde{\boldsymbol{\omega}}_{\mathrm{I},k}$, respectively, the coordinate transformation matrix $(\tilde{\mathbf{C}}_{\mathrm{b}}^{\mathrm{n}})_k$ from the b-frame to the n-frame can be obtained as follows (Grewal et al., 2007):

$$(\tilde{\mathbf{C}}_{\mathrm{b}}^{\mathrm{n}})_k = (\tilde{\mathbf{C}}_{\mathrm{b}}^{\mathrm{n}})_{k-1} \cdot \exp(\tilde{\boldsymbol{\omega}}_{\mathrm{I},k} T_{\mathrm{I}}) = (\tilde{\mathbf{C}}_{\mathrm{b}}^{\mathrm{n}})_{\mathrm{ini}} \cdot \prod_{i=0}^{k} \exp(\tilde{\boldsymbol{\omega}}_{\mathrm{I},i} T_{\mathrm{I}}) \tag{1}$$

where T_{I} denotes the time interval of IMU measurements and $\exp(\cdot)$ denotes the exponential form of the rotation angle (He et al., 2023). $(\tilde{\mathbf{C}}_{\mathrm{b}}^{\mathrm{n}})_{\mathrm{ini}}$ denotes the initial coordinate transformation matrix. By incorporating the non-holonomic constraint and IMU installation constraint, $(\tilde{\mathbf{C}}_{\mathrm{b}}^{\mathrm{n}})_{\mathrm{ini}}$ can be calculated by the heading and pitch angles of the vehicle (R. Sun et al., 2020). Assuming that each calculation

window contains K measurements, the velocity increment $\Delta\tilde{\boldsymbol{v}}_{\mathrm{I},m}$ over the m-th interval can be formulated as follows:

$$\Delta\tilde{\boldsymbol{v}}_{\mathrm{I},m}=\sum_{k=mK}^{(m+1)K-1}\left[(\tilde{\mathbf{C}}_{\mathrm{b}}^{\mathrm{n}})_k\cdot\tilde{\boldsymbol{a}}_{\mathrm{I},k}-\boldsymbol{g}\right]T_{\mathrm{I}}\approx\Delta\boldsymbol{v}_{\mathrm{I},m}+\boldsymbol{\epsilon}_{\mathrm{I},m} \tag{2}$$

where $\boldsymbol{g}$ represents gravity in the n-frame and $\Delta\boldsymbol{v}_{\mathrm{I},m}$ denotes the true velocity increment. $\boldsymbol{\epsilon}_{\mathrm{I},m}$ denotes the measurement noise, which can be assumed as Gaussian noise $\boldsymbol{\epsilon}_{\mathrm{I},m}\sim\mathcal{N}(0,\Sigma_{\mathrm{I}}\approx\sigma_{\mathrm{I}}^2\mathbf{I}_3)$ owing to the approximately linear operation in pre-integration (Wei et al., 2022). $\mathbf{I}_3$ denotes an identity matrix of rank 3.

For GNSS data, the velocity increment measurement $\tilde{\boldsymbol{v}}_{\mathrm{G},m}$ expressed in the n-frame can be directly obtained by the velocity difference:

$$\Delta\tilde{\boldsymbol{v}}_{\mathrm{G},m}=\Delta\boldsymbol{v}_{\mathrm{G},m}+\boldsymbol{\epsilon}_{\mathrm{G},m} \tag{3}$$

where $\Delta\boldsymbol{v}_{\mathrm{G},m}$ denotes the true value and should be equal to $\Delta\boldsymbol{v}_{\mathrm{I},m}$ under spoofing-free scenarios. $\boldsymbol{\epsilon}_{\mathrm{G},m}\sim\mathcal{N}(0,\Sigma_{\mathrm{G}}\approx\mathrm{diag}(\sigma_{\mathrm{G,N}}^2,\sigma_{\mathrm{G,E}}^2,\sigma_{\mathrm{G,D}}^2))$ denotes the measurement noise, where $\mathrm{diag}(\cdot)$ represents the diagonal matrix.

2.2 | Conventional VIDC Spoofing Detection Method

For clarity in our analysis, this derivation focuses on the N-direction of the velocity increment as an example. Within a detection window of M epochs, the velocity increments measured by the IMU and GNSS can be expressed as follows:

$$\begin{aligned}\Delta\tilde{\boldsymbol{v}}_{\mathrm{G}}&=[\Delta\tilde{\boldsymbol{v}}_{\mathrm{G,N},t},\Delta\tilde{\boldsymbol{v}}_{\mathrm{G,N},t+1},\cdots,\Delta\tilde{\boldsymbol{v}}_{\mathrm{G,N},t+M-1}]^{\mathrm{T}}\\\Delta\tilde{\boldsymbol{v}}_{\mathrm{I}}&=[\Delta\tilde{\boldsymbol{v}}_{\mathrm{I,N},t},\Delta\tilde{\boldsymbol{v}}_{\mathrm{I,N},t+1},\cdots,\Delta\tilde{\boldsymbol{v}}_{\mathrm{I,N},t+M-1}]^{\mathrm{T}}\end{aligned} \tag{4}$$

where t denotes the initial epoch. Under spoofing-free conditions, the velocity increments measured by the IMU and GNSS should be consistent with each other, reflecting the physical coherence of the two sensors. However, when spoofing occurs, this consistency is disrupted, as the spoofed GNSS signals intentionally distort the navigation solution. Defining $\nabla\tilde{\boldsymbol{v}}_{\mathrm{IG}}$ as the velocity increment difference between the GNSS and IMU measurements, the conventional spoofing detection hypothesis can be expressed as follows:

$$\begin{aligned}\mathcal{H}_0&:\nabla\tilde{\boldsymbol{v}}_{\mathrm{IG}}=\Delta\tilde{\boldsymbol{v}}_{\mathrm{G}}-\Delta\tilde{\boldsymbol{v}}_{\mathrm{I}}=\boldsymbol{\epsilon}_{\mathrm{IG}}\\\mathcal{H}_1&:\nabla\tilde{\boldsymbol{v}}_{\mathrm{IG}}=\Delta\tilde{\boldsymbol{v}}_{\mathrm{G}}-\Delta\tilde{\boldsymbol{v}}_{\mathrm{I}}=\Delta\boldsymbol{v}_{\mathrm{s}}+\boldsymbol{\epsilon}_{\mathrm{IG}}\end{aligned} \tag{5}$$

where $\mathcal{H}_0$ and $\mathcal{H}_1$ denote spoofing-free and spoofing scenarios, respectively. $\Delta\boldsymbol{v}_{\mathrm{s}}=[\Delta\boldsymbol{v}_{\mathrm{s},t},\cdots,\Delta\boldsymbol{v}_{\mathrm{s},t+M-1}]^{\mathrm{T}}$ denotes the unknown deviations induced by spoofers, which aim to deceive the target receiver into a specific motion state. $\boldsymbol{\epsilon}_{\mathrm{IG}}$ denotes the measurement noise, and it can be assumed that $\boldsymbol{\epsilon}_{\mathrm{IG}}\sim\mathcal{N}(0,\Sigma_{\mathrm{IG}}\approx\sigma_{\mathrm{IG}}^2\mathbf{I}_M)$ and $\sigma_{\mathrm{IG}}^2=\sigma_{\mathrm{I}}^2+\sigma_{\mathrm{G,N}}^2$.

Based on Equation (5), the detection statistics T_{c} can be established according to the Neyman–Pearson criteria (Lo et al., 2017):

$$T_{\mathrm{c}}=\nabla\tilde{\boldsymbol{v}}_{\mathrm{IG}}^{\mathrm{T}}\Sigma_{\mathrm{IG}}^{-1}\nabla\tilde{\boldsymbol{v}}_{\mathrm{IG}}\sim\begin{cases}\mathcal{H}_0:\chi_M^2(0)\\\mathcal{H}_1:\chi_M^2(\lambda_0)\end{cases} \tag{6}$$

where $\chi_n^2(\lambda)$ denotes the chi-square distribution with degree of freedom n and noncentrality parameter λ. The noncentrality parameter λ_c in the above equation can be expressed as follows:

$$\lambda_c = \Delta\boldsymbol{v}_s^T \Sigma_{IG}^{-1} \Delta\boldsymbol{v}_s \tag{7}$$

According to the constant false-alarm rate (CFAR) criteria, the detection threshold τ_0 and decision approach can be written as follows:

$$\tau_c = F_{M,0}^{-1}(1-P_{FA}) \qquad T_c \gtrless_{\mathcal{H}_0}^{\mathcal{H}_1} \tau_c \tag{8}$$

The detection probability $P_{D,c}$ can be obtained based on a preset false-alarm rate P_{FA}:

$$P_{D,c} = 1 - F_{M,\lambda_c}\left(F_{M,0}^{-1}(1-P_{FA})\right) \tag{9}$$

where $F_{n,\lambda}(\cdot)$ and $F_{n,\lambda}^{-1}(\cdot)$ denote the cumulative density function of the chi-square distribution $\chi_n^2(\lambda)$ and its inverse, respectively. These expressions are the basis of the performance comparison presented later.

3 | PROPOSED MM-BASED VIDC SPOOFING DETECTION METHOD

The conventional VIDC approach serves as an intuitive detection method that operates without any prior assumptions on spoofing deviations to reveal the discrepancy between authentic and spoofed motion, offering a relatively high degree of freedom for its detection statistics. However, this characteristic inherently limits its detection performance when dealing with subtle spoofing deviations of vehicular motion states and low-precision vehicle-mounted IMUs. To address these limitations, this paper proposes a novel spoofing detection method based on vehicular motion models to make appropriate constraints on deviations and reduce uncertainty, further improving detection accuracy. The fundamental principles and detection statistics of the proposed MM-based VIDC method will be elaborated in this section.

3.1 | Basic Principle

Kinematic characteristics represent one of the fundamental attributes of vehicles. Commonly recognized motion patterns, such as uniform linear motion and uniformly accelerated motion, can all be expressed using a polynomial motion model $\mathbf{H}_n\boldsymbol{\theta}_n$, using the following mathematical formulation:

$$\mathbf{H}_n = \begin{bmatrix} 1^n & \cdots & 1 & 1 \\ 2^n & \cdots & 2 & 1 \\ \vdots & \vdots & \vdots & \vdots \\ M^n & \cdots & M & 1 \end{bmatrix} \quad \boldsymbol{\theta}_n = \begin{bmatrix} a_n \\ a_{n-1} \\ \vdots \\ a_0 \end{bmatrix} \tag{10}$$

where n represents the model order and M denotes the window length. $\mathbf{H}_n$ denotes the model matrix, $\boldsymbol{\theta}_n$ represents a model parameter, and a_n represents an

n-th-order model coefficient. For example, a first-order velocity increment model describes motion with constant jerk, and a second-order model represents motion with a linear jerk.

In addition, spoofing deviations are determined by not only the vehicle's motion state but also the false motion state induced by the spoofer. To maintain concealment under vehicular scenarios, advanced spoofing-induced motion states typically mimic realistic vehicle motion patterns (Chang, Huang, et al., 2023; Geng et al., 2024). Even if the spoofing source assumes other motion forms such as a stationary or circular trajectory, the motion can still be effectively approximated by motion models over short intervals.

Thus, the deviation $\Delta\boldsymbol{v}_{\mathrm{s}}$ in the presence of spoofing, which equals the discrepancy between the vehicle's authentic motion and the false state preset by the spoofer, can also be effectively characterized by a motion model $\mathbf{H}_n\boldsymbol{\theta}_n$. This theoretical foundation enables a transformation of the original deviation estimation problem in Equation (5) into the following form:

$$\begin{aligned}\mathcal{H}_0 &: \nabla\tilde{\boldsymbol{v}}_{\mathrm{IG}} = \boldsymbol{\epsilon}_{\mathrm{IG}} \\ \mathcal{H}_1 &: \nabla\tilde{\boldsymbol{v}}_{\mathrm{IG}} = \mathbf{H}_n\boldsymbol{\theta}_n + \boldsymbol{\epsilon}_{\mathrm{IG}}\end{aligned} \tag{11}$$

This formulation imposes a theoretically rational constraint on the spoofing deviation $\Delta\boldsymbol{v}_{\mathrm{s}}$ compared with the conventional VIDC method, thereby establishing the mathematical model for our approach. The following subsections will derive its detection statistics and decision-making criterion in detail.

3.2 | Detection Statistics

According to Equation (11), the detector can be established based on the GLRT criterion, which compares the maximum likelihoods of the measurement under the spoofing and spoofing-free hypotheses. The GLRT is a widely used statistical detection framework that achieves excellent performance when certain parameters are unknown (Fan et al., 2001). The likelihood ratio can be expressed as follows:

$$\mathcal{L}\left(\nabla\tilde{\boldsymbol{v}}_{\mathrm{IG}}\right) = \log\frac{p(\nabla\tilde{\boldsymbol{v}}_{\mathrm{IG}};\mathcal{H}_1;\hat{\boldsymbol{\theta}}_n)}{p(\nabla\tilde{\boldsymbol{v}}_{\mathrm{IG}};\mathcal{H}_0)} \tag{12}$$

The maximum likelihood estimation of the n-th-order parameter $\hat{\boldsymbol{\theta}}_n$ can be formulated as follows:

$$\hat{\boldsymbol{\theta}}_n = (\mathbf{H}_n^{\mathrm{T}}\mathbf{H}_n)^{-1}\mathbf{H}_n^{\mathrm{T}}\nabla\tilde{\boldsymbol{v}}_{\mathrm{IG}} \sim \mathcal{N}\left((\mathbf{H}_n^{\mathrm{T}}\mathbf{H}_n)^{-1}\mathbf{H}_n^{\mathrm{T}}\Delta\boldsymbol{v}_{\mathrm{s}}, (\mathbf{H}_n^{\mathrm{T}}\mathbf{H}_n)^{-1}\Sigma_{\mathrm{IG}}\right) \tag{13}$$

By substituting $\hat{\boldsymbol{\theta}}_n$ into the likelihood ratio in Equation (12), the detection statistic T_{m_n} corresponding to the MM-based VIDC method of n-th order can be simplified as follows:

$$T_{\mathrm{m}_n} = \sigma_{\mathrm{IG}}^{-2}\hat{\boldsymbol{\theta}}_n^{\mathrm{T}}\mathbf{H}_n^{\mathrm{T}}\mathbf{H}_n\hat{\boldsymbol{\theta}}_n \sim \begin{cases}\mathcal{H}_0 : \chi^2_{n+1}(0) \\ \mathcal{H}_1 : \chi^2_{n+1}(\lambda_{\mathrm{m}_n})\end{cases} \tag{14}$$

The noncentrality parameter can be derived as follows:

$$\lambda_{\mathrm{m}_n} = \sigma_{\mathrm{IG}}^{-2} \Delta \boldsymbol{v}_{\mathrm{s}}^{\mathrm{T}} \mathbf{H}_n \left(\mathbf{H}_n^{\mathrm{T}} \mathbf{H}_n \right)^{-1} \mathbf{H}_n^{\mathrm{T}} \Delta \boldsymbol{v}_{\mathrm{s}} \tag{15}$$

The threshold and decision-making can also be derived based on the CFAR criterion:

$$\tau_{\mathrm{m}_n} = F_{n+1,0}^{-1}(1 - P_{\mathrm{FA}}) \qquad T_{\mathrm{m}_n} \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \tau_{\mathrm{m}_n} \tag{16}$$

Then, the theoretical detection rate can be calculated:

$$P_{\mathrm{D,m}_n} = 1 - F_{n+1,\lambda_{\mathrm{m}_n}} \left(F_{n+1,0}^{-1}(1 - P_{\mathrm{FA}}) \right) \tag{17}$$

It is evident that the performance of the MM-based VIDC method is contingent upon the parameters λ_{m_n}, which are strongly correlated with specific spoofing deviations. Therefore, the next section will present a detailed analysis of the performance of the MM-based VIDC method under distinct spoofing scenarios and compare its performance with that of the conventional VIDC method.

4 | PERFORMANCE ANALYSIS AND SIMULATION

Based on the derived detector and theoretical performance of the conventional and MM-based VIDC methods, this section presents a comprehensive analysis focused on two aspects. First, we conduct a theoretical comparison based on the concepts of dimension gain and model loss to elucidate the relationship between different methods and deviation scenarios. Subsequently, simulations provide a quantitative validation of our theoretical analysis, showing both the magnitude of performance improvement and the impact of influencing factors.

4.1 | Theoretical Performance Comparison

From the above theoretical results, it can be observed that both the conventional and proposed MM-based VIDC methods yield detection probabilities that follow chi-square distributions. According to the properties of chi-square distributions, a method characterized by a lower degree of freedom and larger noncentrality parameters in Equation (9) and Equation (17) tends to exhibit a superior detection rate under the same P_{FA}. The following analysis qualitatively compares the performance of different methods using the concepts of dimension gain and model loss, providing explanations from both mathematical and physical perspectives. Furthermore, this subsection presents more precise and quantitative results using the first-order MM-based method (denoted as "first-MM") and second-order MM-based method (denoted as "second-MM") as representative examples.

4.1.1 | General Analysis Based on Dimension Gain and Model Loss

The first parameter that critically influences detection performance is the degree of freedom of the chi-square distribution. Dimension gain refers to the improvement

in detection probability achieved by reducing the degrees of freedom, which occurs when MM-based methods employ motion models to reasonably represent spoofing deviations. Specifically, the detection rate of the conventional VIDC method has a degree of freedom M, equal to the data window length, whereas the MM-based VIDC method has a degree of freedom of $n+1$, where $n < M-1$ to avoid overfitting. Therefore, the lower the order of the motion model used in MM-based detection, the fewer the degrees of freedom and, consequently, the greater the dimension gain that enhances detection performance.

The second parameter affecting detection performance is the noncentrality parameter, i.e., λ_{c} and λ_{m_n}. For the conventional approach, the noncentrality parameter $\lambda_{\mathrm{c}} = \sigma_{\mathrm{IG}}^{-2} \Delta \boldsymbol{\nu}_{\mathrm{s}}^{\mathrm{T}} \Delta \boldsymbol{\nu}_{\mathrm{s}}$ in Equation (7) equals the normalized magnitude of the spoofing deviation. However, for MM-based methods, the value of this parameter depends not only on the order n of the detection model but also on the order q of the spoofing deviation, expressed as $\Delta \boldsymbol{\nu}_{\mathrm{s}} = \mathbf{H}_q \boldsymbol{\theta}_q$. Accordingly, two distinct cases are analyzed to investigate their respective impacts on detection performance.

1) Case 1 ($n \geq q$): The detection model order n is no less than the spoofing deviation order q. Based on Equation (10), the relationship between $\mathbf{H}_n$ and $\mathbf{H}_q$ can be determined as follows:

$$\mathbf{H}_q = \mathbf{H}_n \mathbf{Q}_{nq} \quad \text{and} \quad \mathbf{Q}_{nq} = [\mathbf{0}_{q+1,n-q}, \mathbf{I}_{q+1,q+1}]^{\mathrm{T}} \tag{18}$$

where $\mathbf{0}$ and $\mathbf{I}$ denote the null matrix and identity matrix, respectively. Then, the following equation can be derived:

$$\mathbf{H}_q^{\mathrm{T}} \mathbf{H}_n (\mathbf{H}_n^{\mathrm{T}} \mathbf{H}_n)^{-1} \mathbf{H}_n^{\mathrm{T}} \mathbf{H}_q = \mathbf{Q}_{nq}^{\mathrm{T}} \mathbf{H}_n^{\mathrm{T}} \mathbf{H}_n (\mathbf{H}_n^{\mathrm{T}} \mathbf{H}_n)^{-1} \mathbf{H}_n \mathbf{H}_n \mathbf{Q}_{nq} = \mathbf{Q}_{nq}^{\mathrm{T}} \mathbf{H}_n \mathbf{H}_n \mathbf{Q}_{nq} = \mathbf{H}_q^{\mathrm{T}} \mathbf{H}_q \tag{19}$$

Further, the relationship between $\lambda_{\mathrm{c},q}$ and $\lambda_{\mathrm{m}_n,q}$ can be obtained by substituting Equation (19) into Equation (15):

$$\lambda_{\mathrm{m}_n,q} = \sigma_{\mathrm{IG}}^{-2} \Delta \boldsymbol{\nu}_{\mathrm{s}}^{\mathrm{T}} \mathbf{H}_n \left(\mathbf{H}_n^{\mathrm{T}} \mathbf{H}_n \right)^{-1} \mathbf{H}_n^{\mathrm{T}} \Delta \boldsymbol{\nu}_{\mathrm{s}} = \sigma_{\mathrm{IG}}^{-2} \boldsymbol{\theta}_q^{\mathrm{T}} \mathbf{H}_q^{\mathrm{T}} \mathbf{H}_n \left(\mathbf{H}_n^{\mathrm{T}} \mathbf{H}_n \right)^{-1} \mathbf{H}_n^{\mathrm{T}} \mathbf{H}_q \boldsymbol{\theta}_q = \sigma_{\mathrm{IG}}^{-2} \boldsymbol{\theta}_q^{\mathrm{T}} \mathbf{H}_q^{\mathrm{T}} \mathbf{H}_q \boldsymbol{\theta}_q = \lambda_{\mathrm{c},q} \tag{20}$$

The subscript $\mathrm{i} \in \{\mathrm{c}, \mathrm{m}_n\}$ of $\lambda_{\mathrm{i},q}$ identifies the conventional and n-th-order MM-based VIDC method, respectively, and q indicates the spoofing deviation order. Therefore, in this case, it can be observed that the noncentrality parameter $\lambda_{\mathrm{m}_n,q}$ of the MM-based detection probability $P_{\mathrm{D},\mathrm{m}_n,q}$ is identical to $\lambda_{\mathrm{c},q}$ of the conventional method $P_{\mathrm{D},\mathrm{c},q}$. Considering that $P_{\mathrm{D},\mathrm{m}_n,q}$ corresponds to a smaller degree of freedom, the MM-based approach consequently achieves superior detection performance compared with the conventional method. Moreover, as the order of the motion model decreases, the degrees of freedom further decrease, leading to an additional improvement in detection rate.

2) Case 2 ($n < q$): The detection model order n is smaller than the spoofing deviation order q. In this case, $\lambda_{\mathrm{m}_n,q}$ and $\lambda_{\mathrm{c},q}$ are no longer equal. The difference between these two parameters is defined as $\Delta\lambda_{\mathrm{m}_n,q}$, which can be calculated as follows:

$$\Delta\lambda_{\mathrm{m}_n,q} = \lambda_{\mathrm{m}_n,q} - \lambda_{\mathrm{c},q} = \sigma_{\mathrm{IG}}^{-2} \boldsymbol{\theta}_q^{\mathrm{T}} \mathbf{H}_q^{\mathrm{T}} \left[\mathbf{H}_n (\mathbf{H}_n^{\mathrm{T}} \mathbf{H}_n)^{-1} \mathbf{H}_n^{\mathrm{T}} - \mathbf{I} \right] \mathbf{H}_q \boldsymbol{\theta}_q \tag{21}$$

Denoting $\mathbf{B} = \mathbf{H}_n (\mathbf{H}_n^{\mathrm{T}} \mathbf{H}_n)^{-1} \mathbf{H}_n^{\mathrm{T}} - \mathbf{I}$, we can derive $\mathbf{B}^{\mathrm{T}} = \mathbf{B}$ and $\mathbf{B}^2 = -\mathbf{B}$. Thus, all nonzero eigenvalues of $\mathbf{B}$ are equal to -1. The properties determine that matrix $\mathbf{B}$ is a negative semi-definite matrix, leading to a nonpositive β owing

to its quadratic form. Thus, it can be proved that $\Delta\lambda_{\mathrm{m}_n,q} \le 0$, which represents the effect of model loss. According to the derivation shown in Appendix A, $\Delta\lambda_{\mathrm{m}_n,q}$ can be further simplified as follows:

$$\Delta\lambda_{\mathrm{m}_n,q} = \sigma_{\mathrm{IG}}^{-2}\boldsymbol{\theta}_{nq}^{\mathrm{T}}\boldsymbol{\beta}_{nq}\boldsymbol{\theta}_{nq} \quad \text{and} \quad \boldsymbol{\beta}_{nq} = \boldsymbol{\alpha}_{nq}^{\mathrm{T}}\left[\mathbf{H}_n(\mathbf{H}_n^{\mathrm{T}}\mathbf{H}_n)^{-1}\mathbf{H}_n^{\mathrm{T}} - \mathbf{I}\right]\boldsymbol{\alpha}_{nq} \tag{22}$$

where $\boldsymbol{\beta}_{nq}$ is the window factor and $\boldsymbol{\theta}_{nq} = [a_q, \cdots, a_{n+1}]^{\mathrm{T}}$ denotes the high-order coefficients. $\boldsymbol{\alpha}_{nq}$ denotes the difference vector between $\mathbf{H}_q$ and $\mathbf{H}_n$, i.e., $\mathbf{H}_q = [\boldsymbol{\alpha}_{nq}, \mathbf{H}_n]$.

Model loss refers to the degradation in performance caused by a decrease in the noncentrality parameter, which arises from the insufficient representation capacity of the detection model for actual spoofing deviations. Analogous to the underfitting effect, although the MM-based method still benefits from dimension gain in this case, its performance is simultaneously affected by model loss, making the overall relationship between the conventional and MM-based VIDC methods uncertain.

As these two effects, i.e., dimension gain and model loss, exert opposite influences on detection performance, their balance cannot be easily observed from the above theoretical derivations. Therefore, in the following analysis, the first-MM and second-MM are taken as representative examples to provide a more detailed and quantitative discussion.

4.1.2 | *Detailed Analysis Using First-MM and Second-MM as Examples*

To identify a concrete expression of factors influencing the detection performance of different approaches, this section compares the performance of methods based on the first-MM and second-MM (n = 1, 2) under first- and second-order spoofing deviation scenarios ($q = 1, 2$). The first-MM under second-order deviation reflects Case 2 in the above subsection, with other scenarios reflecting Case 1.

Based on the previous theoretical derivations and analysis, the detection probabilities of the MM-based and conventional VIDC methods can be summarized as shown in Table 1. For the subscript notation of $\lambda_{\mathrm{i},q}$ and $P_{\mathrm{D,i},q}$, the index $\mathrm{i} \in \{\mathrm{c}, \mathrm{m}_1, \mathrm{m}_2\}$ identifies the conventional, first-MM-based, and second-MM-based VIDC methods, respectively. $q \in \{1, 2\}$ indicates the spoofing deviation order. The noncentrality parameter difference $\lambda_{\mathrm{m}_1,2}$ of the first-MM under second-order deviation in Table 1 can be expressed in the following form based on the above derivations:

$$\Delta\lambda_{\mathrm{m}_1,2} = \sigma_{\mathrm{IG}}^{-2}\boldsymbol{\theta}_2^{\mathrm{T}}\mathbf{H}_2^{\mathrm{T}}\left[\mathbf{H}_1(\mathbf{H}_1^{\mathrm{T}}\mathbf{H}_1)^{-1}\mathbf{H}_1^{\mathrm{T}} - \mathbf{I}\right]\mathbf{H}_2\boldsymbol{\theta}_2 = \sigma_{\mathrm{IG}}^{-2}a_2^2\beta_{12} \tag{23}$$

where a_2 denotes the second-order coefficient. β_{12} is the window factor, and its explicit expression can be obtained as follows based on derivations in Appendix B:

$$\beta_{12} = -M(M^2-1)(M^2-4)/180 < 0 \ \text{ when } \ M > 2 \tag{24}$$

Thus, the expression of the noncentrality parameter $\lambda_{\mathrm{m}_1,2}$ can be written as follows:

$$\lambda_{\mathrm{m}_1,2} = \lambda_{\mathrm{c},2} + \sigma_{\mathrm{IG}}^{-2}a_2^2\beta < \lambda_{\mathrm{c},2} \tag{25}$$

TABLE 1
Detection Performance of Conventional and MM-Based VIDC Methods Under Distinct Spoofing Deviations

Detection Method	Spoofing Deviation 1: $\Delta\boldsymbol{\nu}_s = \mathbf{H}_1\boldsymbol{\theta}_1$	Spoofing Deviation 2: $\Delta\boldsymbol{\nu}_s = \mathbf{H}_2\boldsymbol{\theta}_2$
Conv	$\lambda_{c,1} = \sigma_{IG}^{-2}\boldsymbol{\theta}_1^T\mathbf{H}_1^T\mathbf{H}_1\boldsymbol{\theta}_1$ $P_{D,c,1} = 1 - F_{M,\lambda_{0,1}}\left(F_{M,0}^{-1}(1-P_{FA})\right)$	$\lambda_{c,2} = \sigma_{IG}^{-2}\boldsymbol{\theta}_2^T\mathbf{H}_2^T\mathbf{H}_2\boldsymbol{\theta}_2$ $P_{D,c,2} = 1 - F_{M,\lambda_{0,2}}\left(F_{M,0}^{-1}(1-P_{FA})\right)$
First-MM	$\lambda_{m_1,1} = \lambda_{c,1}$ $P_{D,m_1,1} = 1 - F_{2,\lambda_{m_1,1}}\left(F_{2,0}^{-1}(1-P_{FA})\right)$	$\lambda_{m_1,2} = \lambda_{c,2} + \Delta\lambda_{m_1,2}$ $P_{D,m_1,2} = 1 - F_{2,\lambda_{m_1,2}}\left(F_{2,0}^{-1}(1-P_{FA})\right)$
Second-MM	$\lambda_{m_2,1} = \lambda_{c,1}$ $P_{D,m_2,1} = 1 - F_{3,\lambda_{m_2,1}}\left(F_{3,0}^{-1}(1-P_{FA})\right)$	$\lambda_{m_2,2} = \lambda_{c,2}$ $P_{D,m_2,2} = 1 - F_{3,\lambda_{m_2,2}}\left(F_{3,0}^{-1}(1-P_{FA})\right)$

The theoretical expressions corresponding to the detection rates of different methods yield two conclusions.

1) Conclusion 1: Under the first-order spoofing deviation scenario, the first-order MM-based VIDC method performs best, followed by the second-order model, with both outperforming the conventional VIDC method. This result occurred because both the first-MM and second-MM can accurately capture the deviation characteristics, resulting in no model loss, while the first-MM provides a higher dimension gain that originates from more precise low-dimensional representations. This relationship is explicable and consistent with the above analysis of Case 1.

2) Conclusion 2: Under the second-order spoofing deviation scenario, the performance advantage of the first-MM depends on the coefficient a_2, which reveals the second-order characteristics of spoofing deviations. When the second-order feature of spoofing deviation is relatively weak (i.e., a_2 is small), the dimension gain advantage of the first-MM method outweighs its minor model loss $\Delta\lambda_{m_1,2}$. However, as a_2 gradually increases, the model loss of the first-MM method also grows, eventually surpassing its dimension gain. This trend causes the detection performance of the first-MM method to decline, becoming lower than that of the second-MM-based method and even the conventional VIDC approach. Consequently, there are two thresholds, i.e., $\hat{a}_{2,s}$ and $\hat{a}_{2,c}$, that determine the performance relationships among the different methods:

$$P_{D,m_1,2} \gtrless P_{D,m_2,2} \text{ if } a_2 \lessgtr \hat{a}_{2,s}, \text{ and } P_{D,m_1,2} \gtrless P_{D,c,2} \text{ if } a_2 \lessgtr \hat{a}_{2,c} \tag{26}$$

These two thresholds can be calculated by solving the equations $P_{D,m_1,2} = P_{D,m_2,2}$ and $P_{D,m_1,2} = P_{D,c,2}$:

$$F_{2,\lambda_{c,2}+\sigma_{IG}^{-2}\beta\hat{a}_{s,2}^2}\left(F_{2,0}^{-1}(1-P_{FA})\right) = F_{3,\lambda_{c,2}}\left(F_{3,0}^{-1}(1-P_{FA})\right) \tag{27}$$

$$F_{2,\lambda_{c,2}+\sigma_{IG}^{-2}\beta\hat{a}_{c,2}^2}\left(F_{2,0}^{-1}(1-P_{FA})\right) = F_{M,\lambda_{c,2}}\left(F_{M,0}^{-1}(1-P_{FA})\right) \tag{28}$$

The solutions are related to the noise level σ_{IG}, window length M, and false-alarm rate P_{FA}. Owing to the higher degree of freedom of the conventional method compared with the second-MM-based method, it can be easily proved that $\hat{a}_{2,c}$ is larger than $\hat{a}_{2,s}$. The detailed numerical values will be shown in Section 4.2. To summarize the results, Table 2 presents a comparative analysis of detection performance across the different methods. The results demonstrate

TABLE 2
Performance Comparison of the Conventional and MM-Based VIDC Methods

$\Delta\boldsymbol{\nu}_s$	Second Coefficient	Conv	First-MM	Second-MM
$\mathbf{H}_1\boldsymbol{\theta}_1$	− − −	worst	best	moderate
$\mathbf{H}_2\boldsymbol{\theta}_2$	$a_2 < \hat{a}_{2,s}$	worst	best	moderate
	$\hat{a}_{2,s} < a_2 < \hat{a}_{2,c}$	worst	moderate	best
	$\hat{a}_{2,c} < a_2$	moderate	worst	best

TABLE 3
Specifications of Fictitious IMU in Simulation

Parameter	Values	Unit
Acc Zero-Bias Instability	1.46×10^{-4}	m/s^2
Acc Random Walk	0.02	$m/s/\sqrt{h}$
Gyr Zero-Bias Instability	10.1	°/h
Gyr Random Walk	0.52	$°/\sqrt{h}$

scenario-dependent performance variations among theMM-based approaches, and the performance of distinct-order MM-based methods depends on the extent to which the spoofing deviations exhibit high-order characteristics. The following subsection provides quantitative simulations to validate our theoretical analysis.

4.2 | Simulation and Influencing Factor Analysis

In this subsection, Monte Carlo simulations are carried out to explore the influencing factors of the MM-based VIDC method and to illustrate quantitative results corresponding to the above analysis. Table 3 lists the specifications of a fictitious IMU that is consistent with the vehicle-mounted IMU used in the following field experiment. IMU data were generated by Aceinna (2019), and spoofing deviations were directly added to authentic GNSS velocity increments to mimic spoofing. As discussed above, the main indicators that affect the detection performance of various methods are the degrees of freedom of the chi-square distribution and noncentrality parameters. The degree of freedom for the MM-based VIDC methods is determined by the detection method itself, whereas the noncentrality parameters encompass all other influencing factors. We define $\Delta\bar{\boldsymbol{\nu}}_s$ as the average spoofing deviation at one epoch, which is written as follows:

$$\Delta\bar{\boldsymbol{\nu}}_s = \sqrt{\Delta\boldsymbol{\nu}_s^{\mathrm{T}}\Delta\boldsymbol{\nu}_s/M} \tag{29}$$

where M denotes the window length and $\Delta\boldsymbol{\nu}_s$ denotes the total spoofing deviation. For example, $\lambda_{c,1}$ can be expressed as follows:

$$\lambda_{c,1} = \sigma_{IG}^{-2}\boldsymbol{\theta}_1^{\mathrm{T}}\mathbf{H}_1^{\mathrm{T}}\mathbf{H}_1\boldsymbol{\theta}_1 = \sigma_{IG}^{-2}\Delta\boldsymbol{\nu}_s^{\mathrm{T}}\Delta\boldsymbol{\nu}_s = \sigma_{IG}^{-2}M(\Delta\bar{\boldsymbol{\nu}}_s)^2 \tag{30}$$

Thus, three influencing factors, including the GNSS noise level σ_G, window length M, and average deviation $\Delta\bar{\boldsymbol{\nu}}_s$, are critical to detection performance. The following subsections present simulation results evaluating the performance of both MM-based and conventional VIDC methods under distinct spoofing scenarios. Each scenario comprises 100,000 Monte Carlo simulation trials.

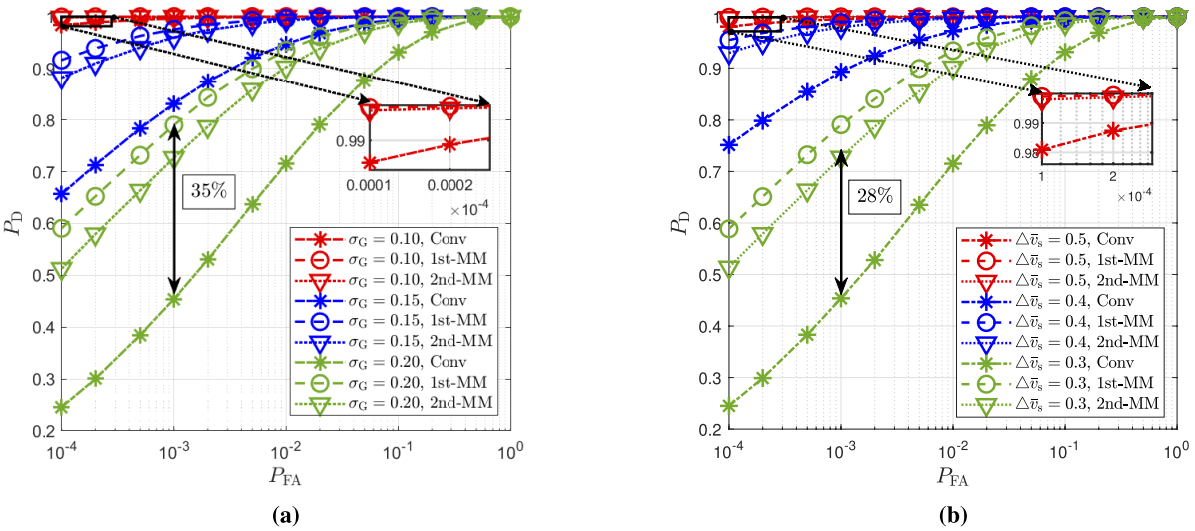


FIGURE 2 First-order deviation: ROC curves for three methods under distinct conditions. (a) Different σ_G values, with $M = 10$ and $\Delta\bar{\boldsymbol{v}}_s = 0.3$ m/s, (b) Different $\Delta\bar{\boldsymbol{v}}_s$ values, with $M = 10$ and $\sigma_G = 0.2$ m/s.

4.2.1 | *Scenario 1: First-Order Deviation*

Figures 2(a) and 2(b) show the receiver operation characteristics (ROC) curves of conventional, first-MM-based, and second-MM-based VIDC methods under first-order deviations, where different scatters of asterisks, circles, and triangles denote the conventional, first-MM-based, and second-MM-based methods, respectively. Curves with distinct colors represent various simulation settings. Both figures illustrate the influence of the GNSS measurement noise level σ_G and average spoofing deviation $\Delta\bar{\boldsymbol{v}}_s$, respectively, showing an obvious increasing trend as σ_G decreases and $\Delta\bar{\boldsymbol{v}}_s$ increases. When $P_{FA} = 0.001$, $\sigma_G = 0.2$ m/s, and $\Delta\bar{\boldsymbol{v}}_s = 0.3$ m/s, which represents normal accuracy (Zhou et al., 2023), the first-MM-based method achieves a detection probability P_D that is roughly 35% higher than that of the conventional method. In comparison, the second-MM-based method demonstrates an approximate 28% enhancement in detection probability over the conventional approach. The first-MM-based method outperforms the second-MM-based method in scenarios involving first-order deviations because it provides a more precise and lower-dimensional representation, verifying Conclusion 1.

4.2.2 | *Scenario 2: Second-Order Deviation*

In this section, we begin by obtaining numerical results for the second-order coefficient thresholds, $\hat{a}_{2,s}$ and $\hat{a}_{2,c}$, as referenced in Equations (27) and (28). These thresholds play crucial roles in determining the relative performance of various methods, as they strike a balance between dimension gain and model loss, which has been analyzed in the previous section.

Figure 3 presents accurate numerical values for different values of the window length M and average spoofing deviation $\Delta\bar{\boldsymbol{v}}_s$. It is obvious that $\hat{a}_{2,c}$ exceeds $\hat{a}_{2,s}$. These two thresholds determine the relative performance levels of the different methods resulting from the balance between dimension gain and model loss. The advantage in dimension gain that the first-MM-based method has over the second-MM-based method is not as pronounced as the advantage it holds over

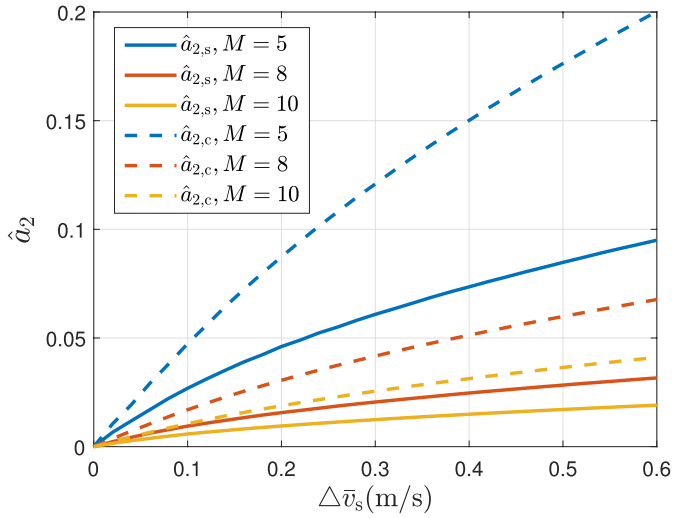
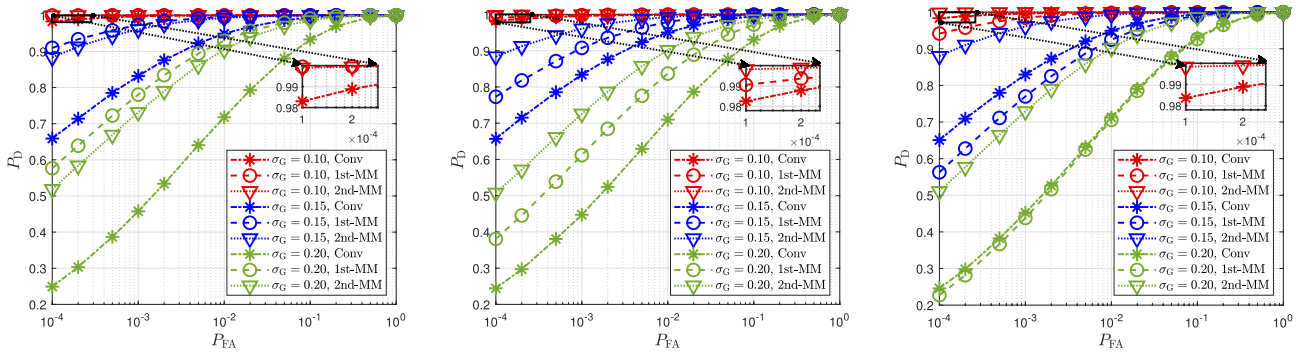


FIGURE 3 Numerical values of second-order coefficient thresholds $\hat{a}_{2,s}$ and $\hat{a}_{2,c}$ under distinct conditions



(a) (b) (c)

FIGURE 4 Second-order deviation: ROC curves for the three methods under different GNSS noise levels with the same window length M = 10 and average deviation $\Delta\bar{\mathbf{v}}_s$ = 0.3 m/s. (a) $a_2 = 0.0077$, (b) $a_2 = 0.0195$, (c) $a_2 = 0.0260$.
Panels (a)–(c) correspond to distinct second-order coefficients, i.e., $a_2 = 0.0077$, 0.0195, and 0.0260, respectively.

the conventional method. Moreover, the model loss of the first-MM, i.e., $\Delta\lambda_{m_1,2}$, increases with the second-order characteristic of spoofing deviation, i.e., a_2. Consequently, the dimension advantage of the first-MM-based method over the conventional method can offset a larger model loss caused by a larger second-order coefficient $\hat{a}_2$, resulting in $\hat{a}_{2,c}$ exceeding $\hat{a}_{2,s}$.

From the horizontal axis perspective, it can be seen that the two thresholds increase with a rise in the average spoofing deviation $\Delta\bar{\boldsymbol{v}}_s$ because a larger spoofing deviation can lead to a larger spoofing noncentrality parameter, which results in an increased dimensionality gain. However, along the vertical axis, it can be seen that thresholds decrease as the window length M increases, although a larger M indicates a larger noncentrality parameter as well. This result is due to the fact that there is a high-order polynomial relationship between the window length factor β and W, as shown in Equation (24), which plays a dominant role in reducing the thresholds.

Figure 4 illustrates the impact of the second-order coefficient a_2 on the performance relationship between the MM-based and conventional methods for the same window length $M = 10$ and average spoofing deviation $\Delta\bar{\boldsymbol{v}}_s = 0.3\,\mathrm{m/s}$.

The second-order coefficients depicted in Figures 4(a)–(c) increase sequentially. Figure 4(a) corresponds to the scenario in which $a_2 = 0.0077$ is less than $\hat{a}_{2,s} = 0.0124$. In this case, the performance of the first-MM is superior to that of the second-MM, and the second-MM outperforms the conventional method. Figure 4(b) corresponds to the situation in which $a_2 = 0.0195$ is greater than $a_{2,s}$ but less than $\hat{a}_{2,c} = 0.0255$. Here, the second-MM demonstrates the best performance, showing obvious improvements over the other two methods. Figure 4(c) presents the case in which $a_2 = 0.0260$ is greater than $a_{2,c}$. In this instance, the performance of the first-MM is even inferior to that of the conventional method. The above simulation results are consistent with Conclusion 2 from our theoretical analysis.

4.2.3 | *Summary*

Based on the aforementioned theoretical derivations and simulations, it can be observed that the MM-based VIDC methods have the potential to outperform the conventional VIDC method in most scenarios. When the average spoofing deviation is 0.3 m/s, the GNSS noise standard deviation is 0.2 m/s, and P_{FA} is 0.001, the performance improvement of the optimal MM-based method can reach approximately 30%. Additionally, the MM-based method with the optimal detection rate strongly depends on the spoofing deviation form and may even lead to performance degradation if the order of the MM-based method is significantly lower than the order of the spoofing deviation model.

5 | FIELD EXPERIMENT

This section presents field experiments to evaluate the performance of the proposed MM-based VIDC method in practical applications. The results validate our theoretical analysis while exploring influencing factors and providing guidance on model order selection for the proposed algorithm.

5.1 | Experiment Settings

Vehicular field experiments were conducted at Tsinghua University on January 16, 2025, at 08:02 Coordinated Universal Time (UTC). Figure 5 illustrates the detailed configurations, including the IMU, GNSS module, and vehicle driving trajectories. The specific parameters of the vehicle-mounted IMU are the same as those listed in Table 3. By collecting vehicular driving data, we obtained total two spoofing data sets, including IMU and GNSS data. The red line represents the authentic trajectory of the vehicle in our experiments, while spoofing signals were directly injected using a remote playback system. The first spoofing data set (ds1) corresponds to a large-deviation spoofing scenario, with the attacker-generated trajectory depicted by a blue curve. The second data set (ds2) characterizes a small-deviation spoofing scenario, generated through a 5-s delay of authentic GNSS signals, with the simulated spoofed trajectory indicated by a green line.

In the field experiments, we uniformly transformed the velocity increments measured by the GNSS and IMU into the navigation frame (n-frame) and utilized the sum of detection statistics in the north and east directions as the detector (Kwon & Shim, 2020). The performance of the different methods will be quantitatively evaluated, comparing the spoofing detection probabilities for a given false-alarm rate.

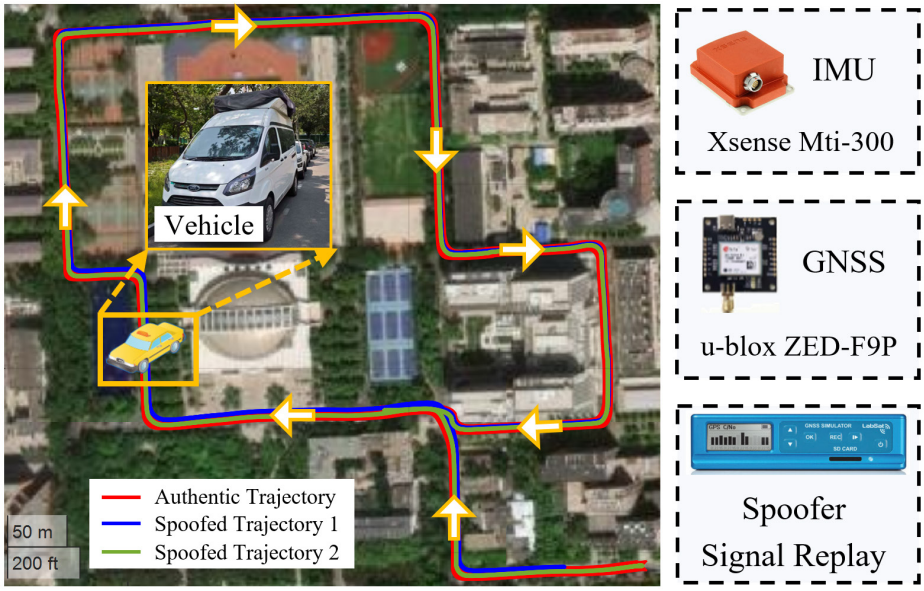


FIGURE 5 Field experiment settings, including equipment and trajectories, corresponding to different scenarios
A u-blox ZED-F9P GNSS receiver and an Xsense Mti-300 IMU module are used to record measurements.

The following analysis will be conducted from two viewpoints, focusing on the improvement of detection performance by the motion models as well as the influence of equivalent driving time.

5.2 | Analysis 1: Detection Performance Enhancement

Figure 6 shows detection statistics for the conventional and MM-based VIDC methods under spoofing and spoofing-free scenarios. It can be seen that all detection statistics fluctuate with time owing to changes in the authentic and spoofed vehicular motion states. The MM-based methods exhibit better effectiveness than the conventional method. Table 4 presents the quantified detection rates exhibited by the different methods for a GNSS frequency of $f_G = 2\,\text{Hz}$ and window length of $M = 10$. Comparing the MM-based methods with the conventional method, it can be observed that the first-MM achieves approximately 45% and 23% higher detection probabilities than the conventional method at a false-alarm rate of 1e-3 in data sets ds1 and ds2, respectively. The performance improvement of the second-MM over the conventional method is 37% and 18%, respectively. These results demonstrate the effectiveness and accuracy of our proposed MM-based algorithm. In addition, it can be found that the performance of the first-MM is superior to that of the second-MM. However, the performance relationship is not fixed and depends on the equivalent driving time, which will be explored in the next subsection.

5.3 | Analysis 2: Influence of Equivalent Driving Time

The equivalent driving time is defined as the duration of a single spoofing detection window. Because spoofing deviations are jointly determined by the vehicle's kinematic behavior and the spoofer's unpredictable state, the exact deviation pattern

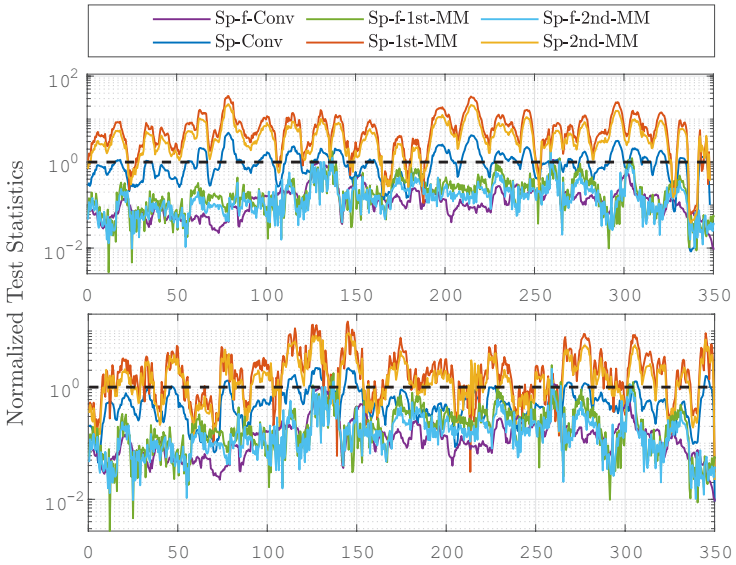


FIGURE 6 Detection statistics of the VIDC and MM-based methods under spoofing (Sp) and spoofing-free (Sp-f) scenarios
The black dashed line represents the logarithmic-normalized threshold with false-alarm rate $P_{FA} = 0.01$. The top and bottom subplots correspond to ds1 and ds2, respectively.

TABLE 4
Detection Rates of the Conventional VIDC and MM-Based VIDC Methods for ds1 and ds2 with $M = 10$ and $f_G = 2$ Hz

Data Set	P_{FA}	Conv	First-MM	Second-MM
ds1	1e-3	32.2%	77.8%	69.8%
	5e-3	36.1%	89.2%	88.6%
	1e-2	43.2%	90.8%	88.9%
ds2	1e-3	8.7%	31.1%	26.2%
	5e-3	9.3%	59.8%	58.3%
	1e-2	11.6%	65.9%	60.8%

within any given driving period is difficult to characterize explicitly. Nevertheless, a fundamental property remains clear: as the equivalent driving time increases, the spoofing deviation is likely to exhibit more high-order components. Table 5 shows the detection performance of the VIDC and MM-based methods of distinct orders under an increasing equivalent driving time T_{eq} for data set ds2. Different window length M values alter the equivalent driving time; for example, T_{eq} is 2.5 s when $M = 5$.

These results allow us to evaluate how the performance gains of MM-based detectors evolve with increasing T_{eq}, and several observations can be made based on Table 5. First, when the equivalent driving time is short (e.g., $M = 5$), the spoofing deviation primarily behaves as a low-order process. In this case, the first-MM achieves the highest detection rates, followed by the zeroth-MM method. This result is consistent with our theoretical finding that the optimal model order aligns with the intrinsic order of the spoofing deviation. The detectors of the second-MM and third-MM exhibit reduced performance due to model loss.

As the equivalent driving time increases, the spoofing deviation exhibits increasingly pronounced higher-order behavior. Correspondingly, higher-order MM-based

TABLE 5
Detection Rates of the Conventional and MM-Based VIDC Methods for Different Equivalent Driving Times for ds2 with $f_G = 2$ Hz

Window M	P_{FA}	Conv	Zeroth-MM	First-MM	Second-MM	Third-MM
$M = 5$ $T_{eq} = 2.5$ s	1e-3	1.9%	13.6%	16.7%	8.1%	6.9%
	5e-3	2.5%	31.3%	34.3%	21.4%	13.6%
	1e-2	7.5%	42.9%	47.3%	24.6%	17.4%
$M = 10$ $T_{eq} = 5$ s	1e-3	8.7%	26.2%	31.1%	26.2%	25.6%
	5e-3	9.3%	37.3%	59.8%	58.3%	45.4%
	1e-2	11.6%	45.0%	65.9%	60.8%	58.6%
$M = 15$ $T_{eq} = 7.5$ s	1e-3	9.3%	22.8%	38.9%	40.4%	40.8%
	5e-3	20.0%	37.7%	58.1%	69.5%	71.6%
	1e-2	20.9%	46.8%	67.7%	75.5%	75.6%

detectors show clear advantages. For instance, when $M = 15$, both the second-MM and third-MM outperform the lower-order methods across all false-alarm levels, aligning with the theoretical conclusion that the model-loss penalty becomes dominant when the detection model order is lower than the true deviation order. This shift in performance ranking with respect to T_{eq} validates the general-order performance relationships derived in Section 4.

In summary, the experimental results confirm the excellent advantages of the proposed MM-based VIDC approach in spoofing detection capacity and validate the performance trends predicted by the theoretical analysis. As the equivalent driving time increases, the spoofing deviation exhibits higher-order characteristics, and the optimal detection performance is achieved by correspondingly higher-order model detectors. These observations demonstrate that selecting an appropriate model order is critical to fully leveraging the advantages of the MM-based framework under different spoofing durations.

5.4 | Analysis 3: Comparison with Other GNSS/IMU Spoofing Detection Methods

To further evaluate the performance gain of the proposed MM-based VIDC approach, two representative GNSS/IMU spoofing detection methods, namely, an innovation-based method and a residual-based method (Crespillo et al., 2017; Khanafseh et al., 2014; Tanıl et al., 2017), were selected for comparison. An EKF-based GNSS/IMU integrated navigation system was constructed, where appropriate process and measurement noise parameters were configured to simulate realistic navigation conditions and avoid bias in the detection rate. Based on this framework, the detection probabilities of different methods were evaluated on two data sets.

Figure 7 illustrates the normalized test statistics of five methods under the ds2, including the conventional VIDC, first-MM-based VIDC, second-MM-based VIDC, innovation-based, and residual-based methods. The statistics are presented for both spoofing scenarios (Sp) and spoofing-free scenarios (Sp-f). It can be observed that all detection statistics exhibit similar temporal trends, while their fluctuation levels vary depending on the detection strategy. In particular, the innovation-based and residual-based methods show only minor differences in their statistics. This behavior is expected because the two methods share the same underlying principle: the

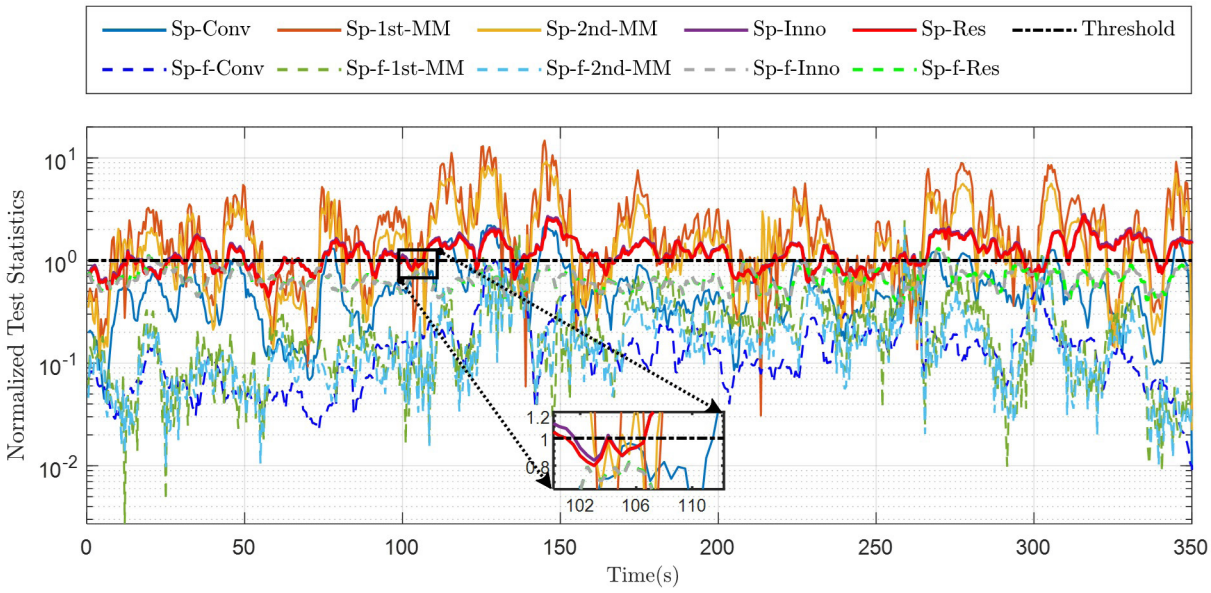


FIGURE 7 Normalized test statistics of the conventional VIDC, MM-based VIDC, innovation-based, and residual-based methods under spoofing (Sp) and spoofing-free (Sp-f) scenarios for data set ds2
The black dashed line represents the logarithmic-normalized threshold with false-alarm rate $P_{FA} = 0.01$.

TABLE 6
Detection Rates of Distinct Methods for ds1 and ds2 with $P_{FA} = 0.01$

Data Set	Window	Conv	First-MM	Second-MM	Inno-Based	Res-Based
ds1	$M = 5$	26.7%	81.9%	72.3%	84.3%	82.3%
	$M = 10$	43.2%	90.8%	88.9%	91.6%	90.4%
	$M = 15$	62.8%	96.4%	96.7%	96.7%	95.2%
ds2	$M = 5$	7.5%	47.3%	24.6%	35.9%	34.9%
	$M = 10$	11.6%	65.9%	60.8%	62.2%	60.1%
	$M = 15$	20.9%	67.7%	75.5%	70.8%	68.3%

innovation-based method utilizes the pre-update states, whereas the residual-based method relies on the post-update states of the EKF.

Table 6 further summarizes the detection probabilities of the compared methods for different detection window lengths. Several observations can be drawn from the results. First, although the residual-based method generally achieves slightly lower detection rates than the innovation-based method, both approaches significantly outperform the conventional VIDC method. This gain is mainly attributed to their ability to exploit temporally accumulated deviation information within the fusion filter.

Second, for data set ds1, which corresponds to relatively large spoofing deviations, the innovation-based method achieves slightly higher detection performance than the MM-based methods. However, for data set ds2, which represents smaller spoofing deviations, the optimal MM-based VIDC model consistently achieves higher detection probabilities than both the innovation-based and residual-based methods. This improvement clearly demonstrates the performance gain introduced by incorporating motion-model constraints. For example, in data set ds2 with $N = 15$, the second-MM-based method achieves the

highest detection probability of 75.5%, which exceeds that of the innovation-based method (70.8%).

These results indicate that the proposed MM-based approach can effectively enhance spoofing detection performance by exploiting simple motion-model characteristics, while still preserving the advantages of the conventional VIDC framework, including compatibility with different GNSS/IMU fusion architectures and low implementation complexity. Such properties make the proposed MM-based VIDC method particularly attractive for practical vehicular navigation anti-spoofing applications.

5.5 | Discussion on Practical Application

The selection of model order is an important practical consideration for applying the proposed MM-based VIDC detection framework. In practice, two strategies can be adopted. A fixed-order approach selects a model order based on expected vehicle motion characteristics and can be chosen conservatively to avoid performance degradation when the true spoofing deviation exhibits higher-order components. For instance, a third-order model ensures robustness across a broad range of lower-order deviation patterns, even though it may not be strictly optimal for lower-order cases. Alternatively, a real-time strategy that determines the model order adaptively may achieve better performance because spoofing deviations in practical scenarios often manifest in a hybrid rather than single-order form. From this perspective, several promising approaches exist for future research, such as adopting Bayesian inference to estimate the dominant deviation structure prior to detection or exploring IMU-assisted approaches to infer suitable model orders. Because such efforts require additional theoretical development involving model-order inference, performance evaluation, and threshold design, this work is identified as an important direction for future research.

Multipath is another practical factor that may affect detection performance. By introducing additional path delays, multipath will increase the noise level of GNSS-derived velocities and may even introduce additional bias. If the influence of multipath only increases the measurement noise level, the resulting false-alarm risk can be mitigated by an appropriate adjustment in the decision threshold. However, severe multipath that induces non-negligible velocity increment bias may lead to false alarms, which is a common limitation of GNSS/IMU-based spoofing detection methods.

6 | CONCLUSION

In this work, we proposed an MM-based VIDC method for detecting GNSS spoofing in IMU-equipped vehicles, aiming to improve the spoofing detection performance of vehicular navigation systems. By incorporating vehicular kinematic characteristics, the proposed approach introduces physically meaningful constraints that reduce the uncertainty of spoofing-induced deviations. A general theoretical framework applicable to arbitrary model orders has been established, and both analytical derivations and simulation results demonstrate that the detection performance is jointly determined by the interplay between dimension gain and model loss. The relationship between the actual order of spoofing deviations and the optimal detection model order has been explicitly characterized. Real-world vehicular experiments further verify the effectiveness of the proposed method with

an enhancement of approximately 30% and demonstrate the performance patterns predicted by theoretical analysis.

ACKNOWLEDGMENTS

This work was supported by the National Natural Science Foundation of China [62473222].

CONFLICT OF INTEREST

The authors declare that they have no known competing interests or personal relationships that could have influenced the work reported in this study.

REFERENCES

Aceinna. (2019). *GNSS-INS-sim*. https://github.com/Aceinna/gnss-ins-sim.git

Broumandan, A., & Lachapelle, G. (2018). Spoofing detection using GNSS/INS/odometer coupling for vehicular navigation. *Sensors, 18*(5), 1305. https://doi.org/10.3390/s18051305

Cao, S., Lu, X., & Shen, S. (2022). GVINS: Tightly coupled GNSS-visual-inertial fusion for smooth and consistent state estimation. *IEEE Transactions on Robotics, 38*(4), 2004–2021. https://doi.org/10.1109/TRO.2021.3133730

Ceccato, M., Formaggio, F., Laurenti, N., & Tomasin, S. (2021). Generalized likelihood ratio test for GNSS spoofing detection in devices with IMU. *IEEE Transactions on Information Forensics Security, 16,* 3496–3509. https://doi.org/10.1109/TIFS.2021.3083414

Chang, J., Huang, F., Zhang, L., Xu, D., & Hsu, L.-T. (2023). Selection of areas for effective GNSS spoofing attacks to a vehicle-mounted MSF system based on scenario classification models. *IEEE Transactions on Vehicular Technology, 72*(11), 14645–14655. https://doi.org/10.1109/TVT.2023.3279831

Chang, J., Zhang, L., Hsu, L.-T., Xu, B., Huang, F., & Xu, D. (2022). Analytic models of a loosely coupled GNSS/INS/LiDAR Kalman filter considering update frequency under a spoofing attack. *IEEE Sensors Journal, 22*(23), 23341–23355. https://doi.org/10.1109/JSEN.2022.3212977

Chang, J., Zhang, Y., Fan, S., Huang, F., Xu, D., & Hsu, L.-T. (2023). An anti-spoofing model based on MVM and MCCM for a loosely-coupled GNSS/INS/LiDAR Kalman filter. *IEEE Transactions on Intelligent Vehicles, 9*(1), 1744–1755. https://doi.org/10.1109/TIV.2023.3335356

Crespillo, O. G., Grosch, A., Skaloud, J., & Meurer, M. (2017, September). Innovation vs residual KF based GNSS/INS autonomous integrity monitoring in single fault scenario. In *Proceedings of the 30th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+)* (pp. 2126–2136). https://doi.org/10.33012/2017.15136

Curran, J. T., & Broumendan, A. (2017, November). On the use of low-cost IMUs for GNSS spoofing detection in vehicular applications. In *Proceedings of International Technical Symposium on Navigation and Timing (ITSNT)* (pp. 1–8).

Dasgupta, S., Rahman, M., Islam, M., & Chowdhury, M. (2022). A sensor fusion-based GNSS spoofing attack detection framework for autonomous vehicles. *IEEE Transactions on Intelligent Transportation Systems, 23*(12), 23559–23572. https://doi.org/10.1109/TITS.2022.3197817

Fan, J., Zhang, C., & Zhang, J. (2001). Generalized likelihood ratio statistics and Wilks phenomenon. *Annals of Statistics,* 153–193.

Gao, C., Wang, G., Shi, W., Wang, Z., & Chen, Y. (2021). Autonomous driving security: State of the art and challenges. *IEEE Internet of Things Journal, 9*(10), 7572–7595. https://doi.org/10.1109/JIOT.2021.3130054

Geng, X., Guo, Y., Tang, K., & Wu, W. (2024). A spoofing algorithm for ground unmanned platform equipped with GNSS/INS integrated navigation system. *IEEE Transactions on Instrumentation and Measurement, 73,* 1–10. https://doi.org/10.1109/TIM.2024.3480222

Grewal, M. S., Weill, L. R., & Andrews, A. P. (2007). *Global positioning systems, inertial navigation, and integration.* John Wiley & Sons.

He, Y., Li, J., & Liu, J. (2023). Research on GNSS INS & GNSS/INS integrated navigation method for autonomous vehicles: A survey. *IEEE Access, 11,* 79033–79055. https://doi.org/10.1109/ACCESS.2023.3299290

Humphreys, T. E. (2013). Detection strategy for cryptographic GNSS anti-spoofing. *IEEE Transactions on Aerospace and Electronic Systems, 49*(2), 1073–1090. https://doi.org/10.1109/TAES.2013.6494400

Jiang, W., Liu, D., Cai, B., Rizos, C., Wang, J., & Shangguan, W. (2019). A fault-tolerant tightly coupled GNSS/INS/OVS integration vehicle navigation system based on an FDP algorithm. *IEEE Transactions on Vehicular Technology, 68*(7), 6365–6378. https://doi.org/10.1109/TVT.2019.2916852

Joubert, N., Reid, T. G., & Noble, F. (2020, October). Developments in modern GNSS and its impact on autonomous vehicle architectures. In *2020 IEEE Intelligent Vehicles Symposium (IV)* (pp. 2029–2036). https://doi.org/10.1109/IV47402.2020.9304840

Kaplan, E. D., & Hegarty, C. (2017). *Understanding GPS/GNSS: Principles and applications.* Artech House.

Khanafseh, S., Roshan, N., Langel, S., Chan, F.-C., Joerger, M., & Pervan, B. (2014, May). GPS spoofing detection using RAIM with INS coupling. In *Proceedings of the IEEE/ION Position, Location and Navigation Symposium (PLANS)* (pp. 1232–1239). https://doi.org/10.1109/PLANS.2014.6851498

Kujur, B., Khanafseh, S., & Pervan, B. (2024). Optimal INS monitor for GNSS spoofer tracking error detection. *NAVIGATION, 71*(1). https://doi.org/10.33012/navi.629

Kwon, K.-C., & Shim, D.-S. (2020). Performance analysis of direct GPS spoofing detection method with AHRS/accelerometer. *Sensors, 20*(4), 954. https://doi.org/10.3390/s20040954

Lee, J.-H., Kwon, K.-C., An, D.-S., & Shim, D.-S. (2015). GPS spoofing detection using accelerometers and performance analysis with probability of detection. *International Journal of Control, Automation and Systems, 13,* 951–959. https://doi.org/10.1007/s12555-014-0347-2

Li, J., Zhu, X., Ouyang, M., Li, W., Chen, Z., & Dai, Z. (2020). Research on multi-peak detection of small delay spoofing signal. *IEEE Access, 8,* 151777–151787. https://doi.org/10.1109/ACCESS.2020.3016971

Liu, Y., Li, S., Fu, Q., Liu, Z., & Zhou, Q. (2019). Analysis of Kalman filter innovation-based GNSS spoofing detection method for INS/GNSS integrated navigation system. *IEEE Sensors Journal, 19*(13), 5167–5178. https://doi.org/10.1109/JSEN.2019.2902178

Lo, S., Chen, Y. H., Reid, T., Perkins, A., Walter, T., & Enge, P. (2017, May). Keynote: The benefits of low cost accelerometers for GNSS anti-spoofing. In *Proceedings of the ION Pacific PNT Meeting* (pp. 775–796). https://doi.org/10.33012/2017.15109

Ma, Y., Li, H., & Lu, M. (2024). Spoofing detection technologies for GNSS/multi-sensor fusion positioning. *Journal of Navigation and Positioning, 12*(4), 114–122. https://doi.org/10.16547/j.cnki.10-1096.20240413

Ma, Y., Wu, Z., Tan, J., Li, X., Lu, M., & Li, H. (2025). Performance analysis and evaluation on GNSS/IMU independent consistency monitoring spoofing detection methods for vehicles. *IEEE Transactions on Vehicular Technology,* 1–15. https://doi.org/10.1109/TVT.2025.3621754

Meng, L., Yang, L., Yang, W., & Zhang, L. (2022). A survey of GNSS spoofing and anti-spoofing technology. *Remote Sensing, 14*(19), 4826. https://doi.org/10.3390/rs14194826

Mina, T., Kanhere, A., Shetty, A., & Gao, G. (2022, September). GPS spoofing-resilient filtering with Chimera and self-contained odometry. In *Proceedings of the 35th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+)* (pp. 3768–3782). https://doi.org/10.33012/2022.18565

Mina, T., Kanhere, A., Shetty, A., & Gao, G. (2024). GPS spoofing-resilient filtering using self-contained sensors and chimera signal enhancement. *NAVIGATION, 71*(2). https://doi.org/10.33012/navi.636

Motella, B., Nicola, M., & Damy, S. (2021). Enhanced GNSS authentication based on the joint CHIMERA/OSNMA scheme. *IEEE Access, 9,* 121570–121582. https://doi.org/10.1109/ACCESS.2021.3107871

Narain, S., Ranganathan, A., & Noubir, G. (2019, May). Security of GPS/INS based on-road location tracking systems. In *2019 IEEE Symposium on Security and Privacy (SP)* (pp. 587–601). https://doi.org/10.1109/SP.2019.00068

Neish, A., Lo, S., Chen, Y.-H., & Enge, P. (2018, September). Uncoupled accelerometer based GNSS spoof detection for automobiles using statistic and wavelet based tests. In *Proceedings of the 31st International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+)* (pp. 2938–2962). https://doi.org/10.33012/2018.15903

Parkinson, B. W., & Axelrad, P. (1988). Autonomous GPS integrity monitoring using the pseudorange residual. *NAVIGATION*, *35*(2), 255–274. https://doi.org/10.1002/j.2161-4296.1988.tb00955.x

Psiaki, M. L., OHanlon, B. W., Powell, S. P., Bhatti, J. A., Wesson, K. D., & Schofield, T. E. (2014, September). GNSS spoofing detection using two-antenna differential carrier phase. In *Proceedings of the 27th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+)* (pp. 2776–2800). https://www.ion.org/publications/abstract.cfm?articleID=12530

Sasani, S., Asgari, J., & Amiri-Simkooei, A. (2016). Improving MEMS-IMU/GPS integrated systems for land vehicle navigation applications. *GPS Solutions, 20,* 89–100. https://doi.org/10.1007/s10291-015-0471-3

Schmittner, C., Griessnig, G., & Ma, Z. (2018, August). Status of the development of ISO/SAE 21434. In *European Conference on Software Process Improvement* (pp. 504–513). https://doi.org/10.1007/978-3-319-97925-0_43

Shang, S., Li, H., Wei, Y., & Lu, M. (2020, January). GNSS spoofing detection and identification based on clock drift monitoring using only one signal. In *Proceedings of the International Technical Meeting of the Institute of Navigation* (pp. 331–340). https://doi.org/10.33012/2020.17147

Sun, C., Cheong, J. W., Dempster, A. G., Demicheli, L., Cetin, E., Zhao, H., & Feng, W. (2018). Moving variance-based signal quality monitoring method for spoofing detection. *GPS Solutions, 22*(3), 83. https://doi.org/10.1007/s10291-018-0745-7

Sun, R., Cheng, Q., & Wang, J. (2020). Precise vehicle dynamic heading and pitch angle estimation using time-differenced measurements from a single GNSS antenna. *GPS Solutions, 24,* 1–9. https://doi.org/10.1007/s10291-020-01000-2

Sun, Y., Li, Z., Yang, Z., Shao, K., & Chen, W. (2022). Motion model-assisted GNSS/MEMS-IMU integrated navigation system for land vehicle. *GPS Solutions, 26*(4), 131. https://doi.org/10.1007/s10291-022-01318-z

Tanıl, Ç., Khanafseh, S., Joerger, M., & Pervan, B. (2017). An INS monitor to detect GNSS spoofers capable of tracking vehicle position. *IEEE Transactions on Aerospace Electronic Systems, 54*(1), 131–143. https://doi.org/10.1109/TAES.2017.2739924

Tanıl, Ç., Khanafseh, S., Joerger, M., & Pervan, B. (2018, September). Sequential integrity monitoring for Kalman filter innovations-based detectors. In *Proceedings of the 31st International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+)* (pp. 2440–2455). https://doi.org/10.33012/2018.15975

Wang, H., Li, H., Zhong, M., & Lu, M. (2024). A space-time-ambiguity decomposition method for DOA estimation enhancing anti-spoofing via rotating dual antennas. *IEEE Transactions on Aerospace Electronic Systems, 60*(6), 7643–7662. https://doi.org/10.1109/TAES.2024.3417434

Wang, L., Chen, L., Li, B., Liu, Z., Li, Z., & Lu, Z. (2024). Development status and challenges of anti-spoofing technology of GNSS/INS integrated navigation. *Frontiers in Physics, 12,* 1425084. https://doi.org/10.3389/fphy.2024.1425084

Wang, L., Ma, Y., Chen, X., Lu, M., & Li, H. (2025, September). A spanning RAIM method with low complexity for GNSS anti-spoofing. In *Proceedings of the 38th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+)* (pp. 1547–1557). https://doi.org/10.33012/2025.20238

Wang, Z., Li, H., Wen, J., & Lu, M. (2021, January). GNSS spoofing discrimination method based on Doppler frequency double difference for multiple independent moving receivers. In *Proceedings of the 2021 International Technical Meeting of the Institute of Navigation* (pp. 56–68). https://doi.org/10.33012/2021.17825

Wei, Y., Li, H., & Lu, M. (2022). A steady-state spoofing detection and exclusion method based on raw IMU measurement. *IEEE Sensors Journal, 22*(4), 3529–3539. https://doi.org/10.1109/JSEN.2022.3143150

Wei, Y., Li, H., Shang, S., & Lu, M. (2020, January). GNSS spoofing detection using raw IMU measurements and pre-integration. In *Proceedings of the International Technical Meeting of the Institute of Navigation* (pp. 626–635). https://doi.org/10.33012/2020.17166

Wu, Z., Zhang, Y., Yang, Y., Liang, C., & Liu, R. (2020). Spoofing and anti-spoofing technologies of global navigation satellite system: A survey. *IEEE Access, 8,* 165444–165496. https://doi.org/10.1109/ACCESS.2020.3022294

Xu, R., Ding, M., Qi, Y., Yue, S., & Liu, J. (2018). Performance analysis of GNSS/INS loosely coupled integration systems under spoofing attacks. *Sensors, 18*(12), 4108. https://doi.org/10.3390/s18124108

Zhang, L., Wang, L., Wu, R., & Zhuang, X. (2024). A new approach for GNSS spoofing detection using power and signal quality monitoring. *Measurement Science and Technology, 35*(12), 126109. https://doi.org/10.1088/1361-6501/ad7629

Zhou, Z., Li, H., Chen, Z., & Lu, M. (2023). Velocity consistency checking based GNSS spoofing detection method for vehicles. *IEEE Transactions on Vehicular Technology, 73*(2), 1974–1990. https://doi.org/10.1109/TVT.2023.3321522

Zhuang, Y., Sun, X., Li, Y., Huai, J., Hua, L., Yang, X., Cao, X., Zhang, P., Cao, Y., & Qi, L. (2023). Multi-sensor integrated navigation/positioning systems using data fusion: From analytics-based to learning-based approaches. *Information Fusion, 95,* 62–90. https://doi.org/10.1016/j.inffus.2023.01.025

How to cite this article: Ma, Y., Lu, M., & Li, H. (2026). A GNSS/IMU spoofing detection method based on motion models for vehicular Navigation. *NAVIGATION*, *73*. https://doi.org/10.33012/navi.789

A | DERIVATION OF NONCENTRALITY PARAMETER DIFFERENCE

The relationship between $\mathbf{H}_q$ and $\mathbf{H}_n$ $(n<q)$ can be written as $\mathbf{H}_q=[\boldsymbol{\alpha}_{nq},\mathbf{H}_n]$, where $\boldsymbol{\alpha}_{nq}$ is expressed as follows:

$$\boldsymbol{\alpha}_{nq}=\begin{bmatrix}1 & 2^q & \cdots & M^q\\ \vdots & \vdots & \vdots & \vdots\\ 1 & 2^{n+1} & \cdots & M^{n+1}\end{bmatrix}^{\mathrm{T}} \tag{31}$$

Based on this relationship, we can derive the following:

$$\mathbf{H}_q^{\mathrm{T}}\mathbf{H}_n=\begin{bmatrix}\boldsymbol{\alpha}_{nq}^{\mathrm{T}}\mathbf{H}_n\\ \mathbf{H}_n^{\mathrm{T}}\mathbf{H}_n\end{bmatrix}\quad\text{and}\quad\mathbf{H}_q^{\mathrm{T}}\mathbf{H}_q=\begin{bmatrix}\boldsymbol{\alpha}_{nq}^{\mathrm{T}}\boldsymbol{\alpha}_{nq} & \boldsymbol{\alpha}_{nq}^{\mathrm{T}}\mathbf{H}_n\\ \mathbf{H}_n^{\mathrm{T}}\boldsymbol{\alpha}_{nq} & \mathbf{H}_n^{\mathrm{T}}\mathbf{H}_n\end{bmatrix} \tag{32}$$

Thus, the noncentrality parameter of an n-th-MM under q-th-order deviation scenarios $\lambda_{\mathrm{m}_n,q}$ can be expressed as follows:

$$\begin{aligned}\lambda_{\mathrm{m}_n,q}&=\sigma_{\mathrm{IG}}^{-2}\boldsymbol{\theta}_q^{\mathrm{T}}\mathbf{H}_q^{\mathrm{T}}\mathbf{H}_n(\mathbf{H}_n^{\mathrm{T}}\mathbf{H}_n)^{-1}\mathbf{H}_n^{\mathrm{T}}\mathbf{H}_q\boldsymbol{\theta}_q\\&=\sigma_{\mathrm{IG}}^{-2}\boldsymbol{\theta}_q^{\mathrm{T}}\begin{bmatrix}\boldsymbol{\alpha}_{nq}^{\mathrm{T}}\mathbf{H}_n\\ \mathbf{H}_n^{\mathrm{T}}\mathbf{H}_n\end{bmatrix}(\mathbf{H}_n^{\mathrm{T}}\mathbf{H}_n)^{-1}[\mathbf{H}_n^{\mathrm{T}}\boldsymbol{\alpha}_{nq};\mathbf{H}_n^{\mathrm{T}}\mathbf{H}_n]\boldsymbol{\theta}_q\\&=\sigma_{\mathrm{IG}}^{-2}\boldsymbol{\theta}_q^{\mathrm{T}}\underbrace{\begin{bmatrix}\boldsymbol{\alpha}_{nq}^{\mathrm{T}}\mathbf{H}_n(\mathbf{H}_n^{\mathrm{T}}\mathbf{H}_n)^{-1}\mathbf{H}_n^{\mathrm{T}}\boldsymbol{\alpha}_{nq} & \boldsymbol{\alpha}_{nq}^{\mathrm{T}}\mathbf{H}_n\\ \mathbf{H}_n^{\mathrm{T}}\boldsymbol{\alpha}_{nq} & \mathbf{H}_n^{\mathrm{T}}\mathbf{H}_n\end{bmatrix}}_{\mathbf{A}_{nq}}\boldsymbol{\theta}_q\end{aligned} \tag{33}$$

The noncentrality parameter difference $\Delta\lambda_{\mathrm{m}_n,q}$ can be further obtained as follows:

$$\begin{aligned}\Delta\lambda_{\mathrm{m}_n,q}&=\lambda_{\mathrm{m}_n,q}-\lambda_{\mathrm{c},q}=\sigma_{\mathrm{IG}}^{-2}\boldsymbol{\theta}_q^{\mathrm{T}}(\mathbf{A}_{nq}-\mathbf{H}_q^{\mathrm{T}}\mathbf{H}_q)\boldsymbol{\theta}_q\\&=\sigma_{\mathrm{IG}}^{-2}\boldsymbol{\theta}_q^{\mathrm{T}}\begin{bmatrix}\boldsymbol{\alpha}_{nq}^{\mathrm{T}}\mathbf{H}_n(\mathbf{H}_n^{\mathrm{T}}\mathbf{H}_n)^{-1}\mathbf{H}_n^{\mathrm{T}}\boldsymbol{\alpha}_{nq}-\boldsymbol{\alpha}_{nq}^{\mathrm{T}}\boldsymbol{\alpha}_{nq} & \mathbf{0}\\ \mathbf{0} & \mathbf{0}\end{bmatrix}\boldsymbol{\theta}_q\\&=\sigma_{\mathrm{IG}}^{-2}\boldsymbol{\theta}_{nq}^{\mathrm{T}}\underbrace{\boldsymbol{\alpha}_{nq}^{\mathrm{T}}\left(\mathbf{H}_n(\mathbf{H}_n^{\mathrm{T}}\mathbf{H}_n)^{-1}\mathbf{H}_n^{\mathrm{T}}-\mathbf{I}\right)\boldsymbol{\alpha}_{nq}}_{\boldsymbol{\beta}_{nq}}\boldsymbol{\theta}_{nq}\end{aligned} \tag{34}$$

where $\boldsymbol{\theta}_{nq}=[a_q,\cdots,a_{n+1}]^{\mathrm{T}}$ and $\boldsymbol{\beta}_{nq}$ is defined as a window factor because it only depends on the window length M.

B | WINDOW FACTOR

To obtain clear expressions of β, the summation n-th power is introduced here to simplify the calculation:

$$S_k=\sum_{i=1}^{M}i^k \tag{35}$$

Thus, we can obtain the following:

$$(\mathbf{H}_1^{\mathrm{T}}\mathbf{H}_1)^{-1} = \frac{1}{S_0S_2 - S_1^2}\begin{bmatrix} S_0 & -S_1 \\ -S_1 & S_1 \end{bmatrix} \tag{36}$$

By substituting the expression of α shown in Equation (31) and simplifying the calculation, we can express β as follows:

$$\beta_{21} = \alpha^{\mathrm{T}}\left[\mathbf{H}_1(\mathbf{H}_1^{\mathrm{T}}\mathbf{H}_1)^{-1}\mathbf{H}_1^{\mathrm{T}} - \mathbf{I}\right]\alpha = \frac{S_0S_3^2 - 2S_1S_2S_3 + S_2^3}{S_0S_2 - S_1^2} - S_4 \tag{37}$$

We utilize the following summation formulas of S_1 to S_4:

$$S_0 = M \quad S_1 = M(M+1)/2 \quad S_2 = M(M+1)(2M+1)/6 \tag{38}$$

$$S_3 = M^2(M+1)^2/4 \quad S_4 = M(M+1)(2M+1)(3M^2+3M-1)/30 \tag{39}$$

Based on the above derivations, β_{21} can be further simplified as follows:

$$\beta = -M(M^2-1)(M^2-4)/180 < 0 \text{ when } M > 2 \tag{40}$$

In practical applications, the detection window length M is usually greater than 2; thus, the window length β_{21} must be negative.