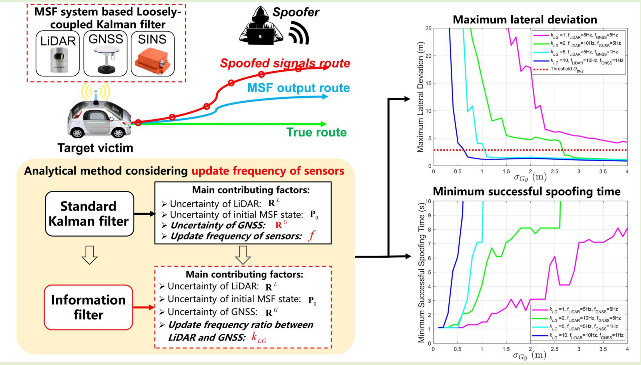
Analytic Models of a Loosely Coupled GNSS/INS/LiDAR Kalman Filter Considering Update Frequency Under a Spoofing Attack

Jiachong Chang, Liang Zhang, *Member, IEEE*, Li-Ta Hsu, *Senior Member, IEEE*, Bing Xu, *Member, IEEE*, Feng Huang, *Graduate Student Member, IEEE*, and Dingjie Xu

***Abstract*—Hostile spoofing attacks on the global navigation satellite system (GNSS) receiver increase the risk of catastrophic consequences to autonomous driving systems. This article addresses the problem of the vulnerability of the Kalman filter (KF) under spoofing attack. A state-of-the-art spoofing attack method based on maximizing the lateral deviation is utilized for verification and analysis. To analyze the vulnerability in actual road scenarios better, an analytic error model of the mechanism of GNSS spoofing is derived. Except for the uncertainty of the initial MSF state, the uncertainty of light detection and ranging (LiDAR), and the uncertainty of GNSS, a new factor in spoofing attacks, the update frequency of different sensors, is investigated in this article, which, in fact, is a key factor to increase the immunity multisensors' fusion (MSF) systems. Experiments were performed in a typical urban scenario of the KAIST dataset. When the update frequency ratios between GNSS and LiDAR are 1, 2, 5, and 10, successful spoof attacks can be performed if the standard deviation (STD) of GNSS is smaller than 4, 2.7, 1.1, and 0.7 m, respectively. Therefore, experiments confirm that the uncertainty of GNSS and the update frequency ratio between LiDAR and GNSS are critical for spoofing attacks, which provides an indication for designing a defense strategy in the future.**


MSF system based Loosely-coupled Kalman filter
LiDAR
GNSS
SINS
Spoofer
Spoofed signals route
MSF output route
True route
Target victim
Analytical method considering update frequency of sensors
Standard Kalman filter
Main contributing factors:
➢ Uncertainty of LiDAR: $\mathbf{R}^L$
➢ Uncertainty of initial MSF state: $\mathbf{P}_0$
➢ Uncertainty of GNSS: $\mathbf{R}^G$
➢ Update frequency of sensors: f
Information filter
Main contributing factors:
➢ Uncertainty of LiDAR: $\mathbf{R}^L$
➢ Uncertainty of initial MSF state: $\mathbf{P}_0$
➢ Uncertainty of GNSS: $\mathbf{R}^G$
➢ Update frequency ratio between LiDAR and GNSS: k_{LG}
Maximum lateral deviation
Maximum Lateral Deviation (m)
σ_{Gy} (m)
k_{LG} =1, f_{LiDAR}=5Hz, f_{GNSS}=5Hz
k_{LG} =2, f_{LiDAR}=10Hz, f_{GNSS}=5Hz
k_{LG} =5, f_{LiDAR}=5Hz, f_{GNSS}=1Hz
k_{LG} =10, f_{LiDAR}=10Hz, f_{GNSS}=1Hz
Threshold D_{th-2}
0
5
10
15
20
25
0
0.5
1
1.5
2
2.5
3
3.5
4
Minimum successful spoofing time
Minimum Successful Spoofing Time (s)
0
1
2
3
4
5
6
7
8
9
10

***Index Terms*—Analytic model, autonomous driving, Kalman filter (KF), multisensors' fusion (MSF), spoofing attack.**

I. Introduction

THE global navigation satellite system (GNSS) plays an irreplaceable role in applications such as cell phones, vehicles, aircraft, and ships [1]. However, GNSS signals are fragile, and the vulnerability arises from two aspects. First, the pseudorandom noise code, the modulation scheme, and the carrier frequency of GNSS civil navigation signals are fully disclosed by the interface control file [2], [3], [4]. Second, the satellite signal propagates over a long distance, so the received signal is extremely weak (about −130 dBm), which is easily influenced by intentional or unintentional interferences [5], [6], [7]. Therefore, the vulnerability of GNSS may lead to security problems [8], [9]. Under a GNSS spoofing attack, the attackers broadcast false satellite signals to the target receiver, intrude into the baseband signal processing blocks of the target receiver, and then deceive the victim to the wrong position [10]. Since the implementation of GNSS spoofing is of low cost, security incidents due to the GNSS spoofing attack are numerous every year [5], [11]. GNSS spoofing deserves great attention because of its strong concealment. Therefore, the research on spoofing and antispoofing of GNSS has become a hot research topic.

Due to the requirements for cost constraints and position accuracy, the inertial navigation system (INS) is generally integrated with GNSS, and light detection and

Manuscript received 8 September 2022; revised 26 September 2022; accepted 3 October 2022. Date of publication 25 October 2022; date of current version 30 November 2022. This work was supported in part by the University Grants Committee of Hong Kong under the scheme Research Impact Fund under Project R5009-21. The associate editor coordinating the review of this article and approving it for publication was Dr. Thilo Sauter. *(Corresponding author: Li-Ta Hsu.)*

Jiachong Chang is with the School of Instrumentation Science and Engineering, Harbin Institute of Technology, Harbin 150001, China, and also with the Department of Aeronautical and Aviation Engineering, The Hong Kong Polytechnic University, Hong Kong (e-mail: jiachong.chang@connect.polyu.hk).

Liang Zhang, Li-Ta Hsu, Bing Xu, and Feng Huang are with the Department of Aeronautical and Aviation Engineering, The Hong Kong Polytechnic University, Hong Kong (e-mail: liang92.zhang@polyu.edu.hk; lt.hsu@polyu.edu.hk; pbing.xu@polyu.edu.hk; darren-f.huang@connect.polyu.hk).

Dingjie Xu is with the School of Instrumentation Science and Engineering, Harbin Institute of Technology, Harbin 150001, China (e-mail: xdj1966@hit.edu.cn).

Digital Object Identifier 10.1109/JSEN.2022.3212977

ranging (LiDAR) for position and navigation in the application of the vehicle localization (VL) systems of autonomous driving vehicles [12], [13], which can reasonably take advantages of each sensor and greatly improve the accuracy of the navigation system. Therefore, a VL system usually establishes a high-precision and high-reliability MSF framework [14], [15], [16], [17] to achieve efficient fusion of several different navigation sensors. In recent years, with the rapid development of the VL system industry, multisensors' fusion (MSF) algorithms based on the Kalman filter (KF) model have been widely used, which can fuse the navigation information of various sensors through recursive formulas to obtain the optimal estimation of the state parameters and, finally, achieve satisfactory position accuracy. Though there are many up-to-date MSF frameworks, including factor graph optimization (FGO) [18], [19], [20], full-source navigation system (FSNS) [21], [22], [23], [24], resilient position navigation and timing (RPNT) [25], [26], AI-based Navigation System [27], [28], [29], and so on, standard loosely coupled KF models are still popular for MSF localization in the practical applications [30], [31], [32]. This is due to the high computing requirement and the high complexity of the latest fusion algorithms.

The problem of GNSS security is increasingly prominent in the MSF algorithm. At present, there are numerous types of research about the generation and identification of GNSS spoofing signals, such as GNSS time synchronization spoofing attacks [33], [34], the GNSS standalone average innovation test [35], physical degradations [36], the vulnerability of GNSS receivers [37], and the impact of target tracking module [38], [39]. These above methods do not involve other navigation sensors. Therefore, some related studies pay more attention to designing spoofing algorithms based on GNSS/INS integrated navigation systems. A covert spoofing method is designed to produce counterfeit global position system (GPS) signals based on tracking control information [40]. A graph model is built for a given road network and enables attackers to derive potential destinations [41]. Correspondingly, many studies focus on defense algorithms. The innovation-based spoofing detection method is applied to loosely coupled GNSS/INS navigation systems [42] and tightly coupled GNSS/INS navigation systems [43]. In addition, a spoofing detection [44] and an exclusion method [45] are developed by integrating the INS. These algorithms are practical for spoof detection in GNSS/INS integrated navigation systems. If the system integrates more sensors, the defense algorithms are more efficient, and the spoofing attack is more difficult to carry out. However, these prior studies are mainly based on GNSS/INS navigation systems and do not provide a detailed analysis of the deceptive GNSS/INS/LiDAR MSF systems, such as the development of the analytic models and the analysis of the error mechanism.

Distinguishing these existing studies, this article focuses on the spoofing attack method for the GNSS/INS/LiDAR MSF systems. Although some factors have been analyzed, such as the measurement uncertainty [9], the update frequency in quantifying the error mechanism has not been considered, which is vital in actual MSF system implementation. Furthermore, due to the relatively low update frequency of GNSS in practical applications, whether other navigation sensors, such as INS and LiDAR, can effectively correct the errors caused by GNSS spoofing is rarely reported. Motivated by these questions, this article conducts in-depth research on the above-unsolved problems, aims to fill the gaps in relevant fields, provides the basis for the spoofing design method of the MSF algorithm, and gives suggestions for anti-GNSS spoofing design.

This article can be summarized from three perspectives. First, we implement a GNSS spoofing attack and introduce a concealed GNSS signal spoofing attack scheme. Following this, we develop an analytical model considering the impact of different sensors' update frequency to analyze the error mechanism of GNSS spoofing behavior. Finally, we use the information filter to establish a simplified analytical model, and then, the results are analyzed clearly.

The main contributions of this article are given as follows.

1) The mechanism of the analytic KF model under a GNSS spoofing attack is presented. Based on the formulas derived, the influences of INS and LiDAR on GNSS spoofing are quantitatively analyzed in one GNSS update cycle. Then, we discovered the main contributing factors to the positioning error, including the uncertainty of the initial MSF state, the uncertainty of LiDAR, the uncertainty of GNSS, and the update frequency of different sensors.
2) We simplify the filter model appropriately by ignoring inconsequential parameters and re-establishing the analytical model via the information filter. Then, we clearly describe the relationship between these significant factors and the state error with this analytical method. We discover that the update frequency ratio between LiDAR and GNSS is also a primary contributing factor to the positioning error under a spoofing attack.
3) We perform experiments using real-world trace data to verify the critical roles of the uncertainty of GNSS and the update frequency ratio between LiDAR and GNSS, which have never been verified under a spoofing attack. Finally, we provide some solutions and directions based on the analytic models to defend against GNSS spoofing attacks.

This article is organized as follows. Section II introduces a loosely coupled GNSS/INS/LiDAR KF MSF algorithm and a state-of-the-art GNSS spoofing attack process. Section III derives an analytic model of standard KF considering sensors' update frequency under a GNSS spoofing attack. Section IV derives the analytic model of the information filter to simplify the measurement update process of the standard KF model. Experiment results verify our conclusions in Section V. Section VI gives suggestions for anti-GNSS spoofing design. Section VII provides the conclusions of this work.

II. Overview of MSF System Under a Spoofing Attack

Aiming at the MSF navigation system based on a loosely coupled KF, this article carries out the research on an

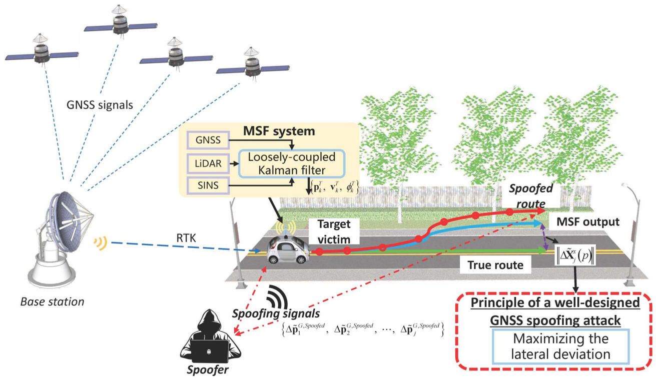

GNSS signals
MSF system
GNSS
LiDAR
SINS
Loosely-coupled
Kalman filter
$\{\mathbf{p}_k^T, \mathbf{v}_k^T, \phi_k^T\}$
Spoofed
route
MSF output
Target
victim
RTK
True route
$\|\Delta\tilde{\mathbf{X}}_j^x(p)\|$
Base station
Spoofing signals
$\{\Delta\tilde{\mathbf{p}}_1^{G,Spoofed}, \Delta\tilde{\mathbf{p}}_2^{G,Spoofed}, \cdots, \Delta\tilde{\mathbf{p}}_j^{G,Spoofed}\}$
Principle of a well-designed
GNSS spoofing attack
Maximizing the
lateral deviation
Spoofer

Fig. 1. VL trajectory changes under an effective GNSS spoofing attack.

aggressive GNSS spoofing attack and explores the influence of GNSS spoofing on the entire navigation system. Fig. 1 describes the change of the VL trajectory under an effective GNSS spoofing attack.

A. MSF Algorithm of a Loosely Coupled GNSS/INS/LiDAR KF [13]

In this article, we use the error-state model to establish the KF state-space model, which has been proven to be effective in the domain of autonomous driving [13]. Before establishing the Kalman state-space model, the Strapdown INS (SINS) kinematic equation and the error equation are required at first, which is introduced in [32]. The SINS state-space model is then established in the loosely coupled KF, including the establishment of the state equation and the measurement equation [46], [47], [48]. The MSF algorithm can fuse the measurements of GNSS and LiDAR with the gyroscope and accelerometer signal of the inertial measurement unit (IMU). Although the update frequency and the navigation precision of sensors are different, the MSF system can also achieve robust state estimation results [49].

1) State Propagation: In most loosely coupled integration systems, the system model of MSF is accurate, and the vehicle (carrier of the sensors) is operated smoothly, which means that it can be assumed that only the bias of the gyroscope and accelerometer needs to be considered [50], [51], [52], [53]. To establish the state equation, the attitude error ϕ, the velocity error $\delta\mathbf{v}^n$, the positioning error $\delta\mathbf{p}$, the accelerometer bias ε^b, and the gyroscope bias ∇^b are selected as state variables in the MSF KF model

$$\mathbf{X} = \begin{bmatrix} \phi^T & (\delta\mathbf{v}^n)^T & (\delta\mathbf{p})^T & (\varepsilon^b)^T & (\nabla^b)^T \end{bmatrix}^T. \qquad (1)$$

The "east-north-upward" (ENU) geographic coordinate system is selected as the navigation coordinate system (n-frame). We also define the body coordinate system (b-frame), the Earth coordinate system (e-frame), and the geocentric inertial coordinate system (i-frame). According to the attitude error, velocity error, and positioning error equations of SINS, the state equation of the KF is constructed. For details, please refer to [30]. Then, a 15-D state equation can be expressed as

$$\dot{\mathbf{X}}(t)_{15\times 1} = \mathbf{F}(t)_{15\times 15}\mathbf{X}(t)_{15\times 1} + \mathbf{G}(t)_{15\times 6}\mathbf{W}(t)_{6\times 1} \qquad (2)$$

where $\mathbf{X}(t)_{15\times 1}$ is the 15-D state variable and

$$\mathbf{F}(t)_{15\times 15} = \begin{bmatrix} \mathbf{M}_{aa}(t) & \mathbf{M}_{av}(t) & \mathbf{M}_{ap}(t) & -\mathbf{C}_b^n & \mathbf{0}_{3\times 3} \\ \mathbf{M}_{va}(t) & \mathbf{M}_{vv}(t) & \mathbf{M}_{vp}(t) & \mathbf{0}_{3\times 3} & \mathbf{C}_b^n \\ \mathbf{0}_{3\times 3} & \mathbf{M}_{pv}(t) & \mathbf{M}_{pp}(t) & \mathbf{0}_{3\times 3} & \mathbf{0}_{3\times 3} \\ \multicolumn{5}{c}{\mathbf{0}_{6\times 15}} \end{bmatrix}$$

is the state transition matrix [32]. $\mathbf{C}_b^n$ is the direction cosine matrix from b-frame to n-frame. $\mathbf{G}(t)_{15\times 6}$ is the state noise transition matrix, which is only related to $\mathbf{C}_b^n$, so it can be ignored [49]. $\mathbf{W}^b = \left[(\mathbf{w}_g^b)^T \quad (\mathbf{w}_a^b)^T\right]^T$ is the state noise. $\mathbf{w}_g^b$ and $\mathbf{w}_a^b$ are the measurement white noise of the gyroscope and accelerometer, respectively.

The system equation of the continuous state-space model is discretized, and the discretization result can be expressed as

$$\mathbf{X}_k = \Phi_{k/k-1}\mathbf{X}_{k-1} + \mathbf{W}_{k-1} \qquad (3)$$

where $\Phi_{k/k-1} \approx \mathbf{I} + ((\mathbf{F}(t_{k-1}))/f_I)$ is the state transition matrix, and f_I is the INS update frequency. We assume that the state noise is white noise, so the mean and variance of the state noise can be expressed as follows:

$$E[\mathbf{W}_k] = 0 \qquad (4a)$$

$$E[\mathbf{W}_k\mathbf{W}_j^T] = \mathbf{Q}\delta_{kj} \qquad (4b)$$

where $\mathbf{Q}$ is the state noise variance matrix. δ_{kj} is the Dirac delta function.

2) Measurement Update: The measurement update process includes LiDAR and GNSS, and the measurement uncertainty is updated. GNSS can provide position information of the vehicle, so INS and GNSS's positioning errors are selected as measurement parameters

$$\mathbf{Z}_1(t)_{3\times 1} = \tilde{\mathbf{p}}_{\text{GNSS}}(t)_{3\times 1} - \tilde{\mathbf{p}}_{\text{INS}}(t)_{3\times 1} \qquad (5)$$

where $\tilde{\mathbf{p}}_{\text{INS}}(t)_{3\times 1}$ is the state update value of INS [30], and $\tilde{\mathbf{p}}_{\text{GNSS}}(t)_{3\times 1}$ is the measurement of GNSS. Then, the measurement update equation can be expressed as

$$\mathbf{Z}_1(t)_{3\times 1} = \mathbf{H}_G(t)_{3\times 15}\mathbf{X}(t)_{15\times 1} + \mathbf{V}^G(t)_{3\times 1} \qquad (6)$$

where $\mathbf{V}^G(t)_{3\times 1}$ is the 3-D measurement noise, and we assume that it follows the Gaussian distribution. The measurement matrix can be expressed as follows:

$$\mathbf{H}_G(t)_{3\times 15} = \begin{bmatrix} \mathbf{0}_{3\times 6} & \mathbf{I}_{3\times 3} & \mathbf{0}_{3\times 6} \end{bmatrix} \qquad (7)$$

where $\mathbf{0}_{3\times 6}$ is a null matrix and $\mathbf{I}_{3\times 3}$ is an identity matrix. The measurement equation is discrete in the actual GNSS/IMU/LiDAR MSF system, so there is no need for discretization. Therefore, when there are GNSS values, the measurement equation of the KF model of the MSF algorithm can be directly expressed as

$$\mathbf{Z}_k = \mathbf{H}_G\mathbf{X}_k + \mathbf{V}_k^G \qquad (8)$$

where $\mathbf{H}_G$ is the measurement matrix and $\mathbf{V}_k^G$ is the measurement noise vector. We assume that the GNSS measurement noise is white noise, and the state noise is not correlated with the measurement noise in the system, so the mean and variance of the measurement noise can be expressed as follows:

$$E\left[\mathbf{V}_k^G\right] = 0 \qquad (9a)$$

$$E\left[\mathbf{V}_k^G\left(\mathbf{V}_j^G\right)^T\right] = \mathbf{R}_G\delta_{kj} \tag{9b}$$

$$E\left[\mathbf{W}_k\left(\mathbf{V}_k^G\right)^T\right] = 0 \tag{9c}$$

where $\mathbf{R}_G$ is the measurement noise covariance matrix, which describes the uncertainty of GNSS measurement values. δ_{kj} is the Dirac delta function.

Here, the result of LiDAR matching with the HD map is used as a measurement of the MSF. We applied [13]. Measurement values are the position and heading angle errors, so positioning errors and heading angle errors of INS and GNSS are selected as measurement parameters

$$\mathbf{Z}_2(t)_{4\times 1} = \begin{bmatrix} \widetilde{\mathbf{p}}_{\text{LiDAR}}(t)_{3\times 1} - \widetilde{\mathbf{p}}_{\text{INS}}(t)_{3\times 1} \\ \phi_{U_L}(t) - \phi_{U_I}(t) \end{bmatrix} \tag{10}$$

where $\widetilde{\mathbf{p}}_{\text{LiDAR}}(t)_{3\times 1}$ is the measurement of LiDAR, $\phi_{U_L}(t)$ and $\phi_{U_I}(t)$ are the heading angle of LiDAR and IMU, and then, the measurement update equation can be expressed as

$$\mathbf{Z}_2(t)_{4\times 1} = \mathbf{H}_L(t)_{4\times 15}\mathbf{X}(t)_{15\times 1} + \mathbf{V}_L(t)_{4\times 1} \tag{11}$$

where $\mathbf{V}_L(t)_{4\times 1}$ is a 4-D measurement noise, and we assume that it follows the Gaussian distribution. We unify the measurement values of LiDAR into the n-system so that the measurement matrix can be expressed

$$\mathbf{H}_L(t)_{4\times 15} = \begin{bmatrix} \mathbf{0}_{3\times 6} & \mathbf{C}_b^n & \mathbf{0}_{3\times 6} \\ \mathbf{C}_b^{n(3,:)} & 0_{1\times 3} & \mathbf{0}_{1\times 6} \end{bmatrix}. \tag{12}$$

When there is LiDAR measurement, the measurement equation of the KF model of the MSF algorithm can be directly expressed as

$$\mathbf{Z}_k = \mathbf{H}_L\mathbf{X}_k + \mathbf{V}_k^L \tag{13}$$

where $\mathbf{H}_L$ is the measurement matrix and $\mathbf{V}_k^L$ is the measurement noise vector. Assume that the LiDAR measurement noise is white noise, and the state noise is not correlated with the measurement noise in the MSF system, so the mean and variance of the measurement noise can be expressed as

$$E\left[\mathbf{V}_k^L\right] = 0 \tag{14a}$$

$$E\left[\mathbf{V}_k\left(\mathbf{V}_j^L\right)^T\right] = \mathbf{R}_L\delta_{kj} \tag{14b}$$

$$E\left[\mathbf{W}_k\left(\mathbf{V}_k^L\right)^T\right] = 0 \tag{14c}$$

where $\mathbf{R}_L$ is the measurement noise covariance matrix that describes the uncertainty of LiDAR measurement values. δ_{kj} is the Dirac delta function.

In the loosely coupled standard KF, the state estimation results do not influence the system covariance matrix since there is no const tuning process [13], so the GNSS spoofing attack does not lead to the change of the system covariance matrix [9].

B. State-of-the-Art GNSS Spoofing Attack Process for MSF System [9]

Due to the anti-interference ability of the MSF system itself, under the condition of the chi-square test [54], [55], [56], [57] (the MSF system of the vehicle typically has a specific resistance to outliers), it could prevent temporary or accidental failures. The innovation of KF can be expressed as

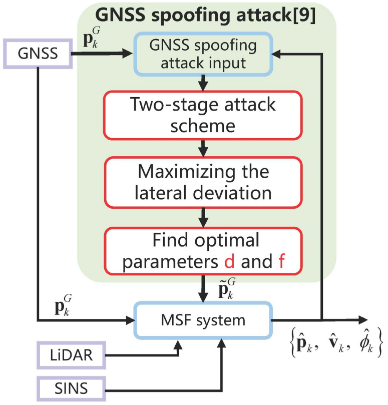

GNSS spoofing attack[9]
GNSS
$\mathbf{p}_k^G$
GNSS spoofing attack input
Two-stage attack scheme
Maximizing the lateral deviation
Find optimal parameters d and f
$\widetilde{\mathbf{p}}_k^G$
$\mathbf{p}_k^G$
MSF system
$\{\hat{\mathbf{p}}_k, \hat{\mathbf{v}}_k, \hat{\phi}_k\}$
LiDAR
SINS

Fig. 2. Illustration of a state-of-the-art GNSS spoofing attack scheme.

$$\gamma_k = \mathbf{Z}_k - \mathbf{H}_k\mathbf{X}_k \tag{15}$$

where γ_k is the innovation at epoch k, $\mathbf{Z}_k$ is the observation, and $\mathbf{X}_k$ is the priority estimated error vector. Under normal conditions, γ_k obeys a Gaussian distribution of zero mean, and its covariance matrix is

$$\mathbf{S}_k = \mathbf{H}_k\mathbf{P}_{k/k-1}\mathbf{H}_k^T + \mathbf{R}_k. \tag{16}$$

According to the statistical properties of innovation sequence, the statistics defined by the following equation follow a χ^2 distribution with m degrees of freedom:

$$\gamma_k^T\mathbf{S}_k^{-1}\gamma_k \sim \chi^2(m) \tag{17}$$

where m is the dimension of the measurement vector. The spoofing detection can be summarized into a hypothesis test as follows:

$$T_D = \chi^2_{1-P_M}(m) \tag{18}$$

where T_D is a statistical significance threshold, which can be obtained by checking the χ^2 distribution table. P_M is the required false alarm rate, and $P_M = 1 - \alpha$, where α is the tail probability and $p\{\chi^2(m) > \chi^2_\alpha(m)\} = \alpha$ [58]. If the chi-square test value is larger than T_D, the measurement will be treated as an outlier.

However, well-designed GNSS spoofing attack schemes can make full use of the inherent defects of the MSF system so that the defensive measures may ignore these GNSS spoofing attack schemes. A state-of-the-art GNSS spoofing attack scheme is shown in Fig. 2. In order to facilitate the quantification of the spoofing attack model, the assumptions listed below are made. We follow the implementation and the assumptions made by [9].

1) The GNSS attackers can detect the vehicle's true position and velocity information in real time.
2) The GNSS attackers can deceive the GNSS signals and completely replace the original GNSS signals of the victim.

3) GNSS spoofing attacks are implemented when the vehicle travels straight ahead at a constant velocity.
4) The maximum attack time that a spoofer can perform a GNSS spoofing attack is limited.
5) The spoofing activity is consistent with a false position, and the spoofer model is a trans-receiver spoofer model [59].

Assume that the maximum number of GNSS epochs that the attackers can implement is

$$k_{\max}^{\text{Spoof}} = T_{\max}^{\text{Spoof}} \cdot f_G \tag{19}$$

where f_G is the GNSS update frequency and $T_{\max}^{\text{Spoofed}}$ is the maximum attack time. Generally, the GNSS spoofing behavior is given a fixed deviation $\Delta\widetilde{\mathbf{p}}_j^{G,\text{Spoofed}}$. Therefore, the implementation of a deceived GNSS sequence (the first to the jth epoch) can be given as

$$\left\{\Delta\widetilde{\mathbf{p}}_1^{G,\text{Spoofed}}, \Delta\widetilde{\mathbf{p}}_2^{G,\text{Spoofed}}, \dots, \Delta\widetilde{\mathbf{p}}_j^{G,\text{Spoofed}}\right\}, \quad j \le k_{\max}^{\text{Spoof}}. \tag{20}$$

Then, the GNSS measurement value is spoofed and becomes

$$\widetilde{\mathbf{p}}_j^G = \mathbf{p}_j^G + \Delta\widetilde{\mathbf{p}}_j^{G,\text{Spoofed}}, \quad j = 1, 2, \dots \text{ and } j \le k_{\max}^{\text{Spoof}} \tag{21}$$

where $\widetilde{\mathbf{p}}_j^G$ is the position information provided by the spoofing attacker. $\mathbf{p}_j^G$ is the real position of the vehicle. $\Delta\widetilde{\mathbf{p}}_j^{G,\text{Spoofed}} = [\Delta\widetilde{L}_j \quad \Delta\widetilde{\lambda}_j \quad 0]^T$ is the attack value in the n-frame. Assume that $\Delta\widetilde{\mathbf{X}}_j(p) = [\Delta\widetilde{\mathbf{X}}_j^x(p) \quad \Delta\widetilde{\mathbf{X}}_j^y(p) \quad 0]^T$ is the output deviation of the MSF system due to the spoofing attack, where $\Delta\widetilde{\mathbf{X}}_j^x(p)$ is the lateral deviation expected to be generated after the spoofing attack and $\Delta\widetilde{\mathbf{X}}_j^y(p)$ is the vertical deviation.

The spoofing attack scheme is divided into two stages. Stage-1 is the constant value attack, and the purpose is to find the vulnerable period of the MSF system, that is, the LiDAR positioning reliability is low, and the GNSS positioning reliability is high. In this stage, the constant attack parameter is

$$\begin{aligned} d &= \left\|\mathbf{C}_n^b \cdot \Delta\widetilde{\mathbf{p}}_j^{G,\text{Spoofed}}\right\| \\ \text{s.t. } &\left\|\Delta\widetilde{\mathbf{X}}_j^x(p)\right\| < D_{\text{th-1}} \end{aligned} \tag{22}$$

where d is the constant value parameter of the attacker. $\mathbf{C}_n^b$ is the direction cosine matrix from n-frame to b-frame. $\|\bullet\|$ is the process of modular arithmetic. $D_{\text{th-1}}$ is the threshold of Stage-1. The purpose of Stage-1 is to find the vulnerable period of the MSF system, and we calculate $D_{\text{th-1}}$ via the width of the lane line and the vehicle's width

$$D_{\text{th-1}} = \frac{L - C}{2} \tag{23}$$

where L represents the width of the lane and C represents the width of the vehicle. When the lateral deviation exceeds $D_{\text{th-1}}$, as shown in Fig. 3, the vehicle will hit the lane line under the GNSS spoofing attack. Thus, when the lateral deviation exceeds $D_{\text{th-1}}$, the spoofing attack will enter Stage-2, which is an exponential value attack scheme. It means that the vulnerability period is found, and the attacker can perform an exponential spoofing attack, triggering the take-over effect [9] and quickly completing the spoofing process

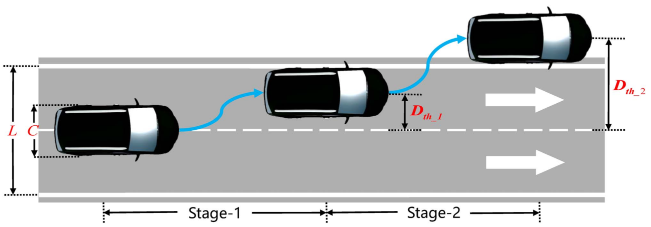


Fig. 3. Diagram for threshold calculation of $D_{\text{th-1}}$ and $D_{\text{th-2}}$.

$$\begin{aligned} d \cdot f^\tau &= \left\|\mathbf{C}_n^b \cdot \Delta\widetilde{\mathbf{p}}_j^{G,\text{Spoofed}}\right\| \\ \text{s.t. } &\left\|\Delta\widetilde{\mathbf{X}}_j^x(p)\right\| > D_{\text{th-1}} \end{aligned} \tag{24}$$

where f is the exponential value parameter of the attacker. τ is the exponential value attack epoch. If the lateral deviation exceeds the threshold $D_{\text{th-2}}$, the spoofing attack is successful

$$\left\|\Delta\widetilde{\mathbf{X}}_j^x(p)\right\| \ge D_{\text{th-2}}. \tag{25}$$

Then, the exponential spoofing attack has created a risk that the vehicle will drive out of the entire lane. Finally, we also calculate $D_{\text{th-2}}$ via the width of the lane line and the vehicle's width

$$D_{\text{th-1}} = \frac{L + C}{2}. \tag{26}$$

The principle of a state-of-the-art GNSS spoofing attack scheme is to maximize the lateral deviation of the vehicle and find the corresponding parameters d and f while satisfying the basic conditions. The deviation generated each time cannot be detected by the chi-square test. The deception time in the actual process is limited under the condition of a finite spoofing sequence

$$\begin{aligned} \{d, f\} &= \mathcal{M}\left\{\left\|\Delta\widetilde{\mathbf{X}}_j^x(p)\right\|\right\} \\ &\text{s.t. } \chi_j^2 < \chi_{\text{Threshold}}^2 \\ &\text{s.t. } j \le k_{\max}^{\text{Spoof}} \end{aligned} \tag{27}$$

where $\mathcal{M}\{\bullet\}$ is the calculative process to find the parameters d and f when the lateral deviation is maximal, χ_j^2 is the jth epoch value of the chi-square test, and $\chi_{\text{Threshold}}^2$ is the threshold value of the chi-square test.

III. Analytic Model of Standard KF Considering Update Frequency Under a GNSS Spoofing Attack

To discover the main contributing factors to the state error through a detailed KF derivation process, other than the tuning of $\mathbf{Q}$ and $\mathbf{R}$, this article takes one more step to consider the impact caused by different sensors' update frequency. In the GNSS/LiDAR/INS MSF framework, the sensors' update frequency is generally different, as shown in Fig. 4. For example, the GNSS update frequency f_G is 1 or 5 Hz, the LiDAR update frequency f_L is 5 or 10 Hz, the INS update frequency f_I

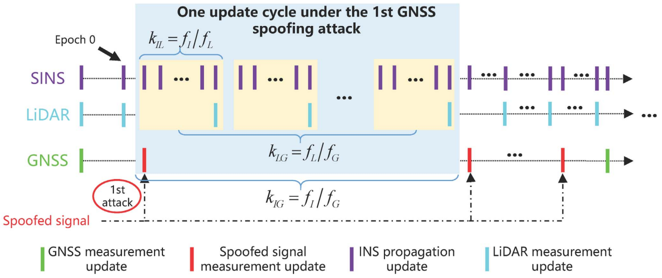


Fig. 4. KF update process considering sensors' update frequency.

is 100, 200, or 400 Hz, and, in general, $f_G \le f_L < f_I$. For convenience, the update frequency can be expressed as

$$k_{IL} = f_I/f_L \tag{28a}$$

$$k_{IG} = f_I/f_G \tag{28b}$$

$$k_{LG} = f_L/f_G. \tag{28c}$$

The epoch bases on SINS, and there are some epochs of GNSS updates and LiDAR updates. Moreover, our purpose is to find the main contributing factors to positioning errors under aggressive spoofing attacks rather than considering the question of time synchronization. In fact, all the sensors are synchronous before we perform the MSF algorithm, so we assume that the measurements of GNSS, LiDAR, and INS are fully synchronous in the process of mathematical derivation.

A. Error Analysis of GNSS Measurement Update Process

Assume that the LiDAR measurement has just been updated at epoch 0, and then, a GNSS signal exists at epoch 1. According to the KF recursive formula of the state propagation, the state prediction values and the one-step covariance matrix can be expressed as

$$\hat{\mathbf{X}}_{1/0} = \Phi_{1/0}\hat{\mathbf{X}}_0 \tag{29a}$$

$$\mathbf{P}_{1/0} = \Phi_{1/0}\mathbf{P}_0\Phi_{1/0}^T + \mathbf{Q} \tag{29b}$$

where $\Phi_{1/0}$ is the initial state transition matrix. $\mathbf{P}_0$ is the initial covariance matrix, which indicates the uncertainty of the initial MSF state. If the GNSS signal is not spoofed, the measurement update equation after the state update is

$$\hat{\mathbf{X}}_1 = \hat{\mathbf{X}}_{1/0} + \mathbf{K}_1(\mathbf{Z}_1 - \mathbf{H}_G\hat{\mathbf{X}}_{1/0}) \tag{30}$$

where the gain matrix and covariance matrix of the KF can be expressed as

$$\mathbf{K}_1 = \mathbf{P}_{1/0}\mathbf{H}_G^T\left(\mathbf{H}_G\mathbf{P}_{1/0}\mathbf{H}_G^T + \mathbf{R}_G\right)^{-1} \tag{31a}$$

$$\mathbf{P}_1 = (\mathbf{I} - \mathbf{K}_1\mathbf{H}_G)\mathbf{P}_{1/0} \tag{31b}$$

where $\mathbf{R}_G$ is the measurement noise covariance matrix that describes GNSS measurement values' uncertainty. Assume that the vehicle is running on the road, the motion state is stable, and the system noise characteristics remain unchanged. When the GNSS position information is spoofed, there will be a positioning error, so the measurement value of GNSS position information is $\widetilde{\mathbf{p}}_j^G$ due to the attacker. If there is no spoofing attack, the measured value of GNSS position information is $\mathbf{p}_j^G$. Then, the relationship between the two values is satisfied

$$\widetilde{\mathbf{p}}_j^G = \mathbf{p}_j^G + \Delta\widetilde{\mathbf{p}}_j^{G,\text{Spoofed}} \tag{32}$$

where $\Delta\widetilde{\mathbf{p}}_j^{G,\text{Spoofed}} = \left[\Delta\widetilde{L}_j \ \Delta\widetilde{\lambda}_j \ 0\right]^T$ is the increment of the spoofing position added to the real GNSS signal and j is the spoofing attack sequence, so the relationship between the spoofed measurement value $\widetilde{\mathbf{Z}}_1$ and the actual measurement value $\mathbf{Z}_1$ at epoch 1 is

$$\widetilde{\mathbf{Z}}_1 = \mathbf{Z}_1 + \Delta\widetilde{\mathbf{p}}_1^{G,\text{Spoofed}}. \tag{33}$$

The deceived measurement update value is

$$\widetilde{\mathbf{X}}_1 = \hat{\mathbf{X}}_{1/0} + \mathbf{K}_1^G(\widetilde{\mathbf{Z}}_1 - \mathbf{H}_G\hat{\mathbf{X}}_{1/0}). \tag{34}$$

As we can see, the gain matrix and the covariance matrix of the KF are identical. Then, the state error caused by GNSS spoofing can be expressed as

$$\Delta\widetilde{\mathbf{X}}_1 = \widetilde{\mathbf{X}}_1 - \hat{\mathbf{X}}_1. \tag{35}$$

The state error after the GNSS spoofing can be further obtained

$$\Delta\widetilde{\mathbf{X}}_1 = \mathbf{K}_1 \cdot \Delta\widetilde{\mathbf{p}}_1^{G,\text{Spoofed}}. \tag{36}$$

B. Error Analysis of IMU State Propagation Process

Due to GNSS having just been updated and the update frequency of LiDAR being generally higher than the update frequency of GNSS, there is no position measurement of GNSS and LiDAR until epoch k_{IL}. Therefore, there is only a state propagation process with INS information in the KF. The state prediction and the one-step covariance matrix can be expressed as

$$\widetilde{\mathbf{X}}_{2/1} = \Phi_{2/1}\widetilde{\mathbf{X}}_1 \tag{37a}$$

$$\mathbf{P}_{2/1} = \Phi_{2/1}\mathbf{P}_1\Phi_{2/1}^T + \mathbf{Q}. \tag{37b}$$

Since there is no measurement update process, the final state update result and the covariance matrix can be expressed as

$$\widetilde{\mathbf{X}}_2 = \widetilde{\mathbf{X}}_{2/1} \tag{38a}$$

$$\mathbf{P}_2 = \mathbf{P}_{2/1}. \tag{38b}$$

Then, the state recursive estimation results and the covariance matrix before the update of LiDAR measurements are

$$\widetilde{\mathbf{X}}_{k_{IL}+1/k_{IL}} = \prod_{\eta=1}^{k_{IL}} \Phi_{\eta+1/\eta} \cdot \widetilde{\mathbf{X}}_1 \tag{39a}$$

$$\mathbf{P}_{k_{IL}+1/k_{IL}} = \Phi_{k_{IL}+1/k_{IL}} \cdot \mathbf{P}_{k_{IL}} \cdot \Phi_{k_{IL}+1/k_{IL}}^T + \mathbf{Q} \tag{39b}$$

where η is the state propagation sequence. If there is no GNSS spoofing attack, the covariance matrix is unchanged, and the state recursive estimation results can be expressed as

$$\hat{\mathbf{X}}_{k_{IL}+1/k_{IL}} = \prod_{\eta=1}^{k_{IL}} \Phi_{\eta+1/\eta} \cdot \hat{\mathbf{X}}_1. \tag{40}$$

The difference between the state update result $\Delta\widetilde{\mathbf{X}}_{k_{IL}+1/k_{IL}}$ before and after the spoofing attack can be expressed as

$$\Delta\widetilde{\mathbf{X}}_{k_{IL}+1/k_{IL}} = \widetilde{\mathbf{X}}_{k_{IL}+1/k_{IL}} - \hat{\mathbf{X}}_{k_{IL}+1/k_{IL}}. \tag{41}$$

Therefore, the state error caused by the GNSS spoofing attack can be expressed as

$$\Delta\widetilde{\mathbf{X}}_{k_{IL}+1/k_{IL}} = \prod_{\eta=1}^{k_{IL}} \Phi_{\eta+1/\eta} \cdot \Delta\widetilde{\mathbf{X}}_1. \tag{42}$$

Assuming that the vehicle is moving relatively smoothly, the state can be regarded as constant in an INS update time, so the system matrix can be assumed constant. Then, $\Phi_{\eta+1/\eta} \approx \mathbf{I} + (\mathbf{F}_0/f_I) = \Phi_{1/0}$, $\eta = 1, \ldots, k_{IL}$

$$\Delta\widetilde{\mathbf{X}}_{k_{IL}+1/k_{IL}} \approx \left(\Phi_{1/0}\right)^{k_{IL}} \cdot \Delta\widetilde{\mathbf{X}}_1 \tag{43}$$

so

$$\Delta\widetilde{\mathbf{X}}_{k_{IL}+1/k_{IL}} \approx \left[\mathbf{I} + \frac{\mathbf{F}_0}{f_I}\right]^{k_{IL}} \cdot \Delta\widetilde{\mathbf{X}}_1. \tag{44}$$

Expand the above equation binomially

$$\Delta\widetilde{\mathbf{X}}_{k_{IL}+1/k_{IL}} = \left[\mathbf{I} + C_{k_{IL}}^1 \cdot \frac{\mathbf{F}_0}{f_I} + C_{k_{IL}}^2 \cdot \left(\frac{\mathbf{F}_0}{f_I}\right)^2 + \cdots + C_{k_{IL}}^{k_{IL}} \cdot \left(\frac{\mathbf{F}_0}{f_I}\right)^{k_{IL}}\right] \cdot \Delta\widetilde{\mathbf{X}}_1 \tag{45}$$

where $C_{k_{IL}}^{\eta}$ is the binomial coefficient, which can be expressed as

$$C_{k_{IL}}^{\eta} = \frac{k_{IL}!}{\eta!\,(k_{IL}-\eta)!}. \tag{46}$$

Then, we simplify the results

$$\Delta\widetilde{\mathbf{X}}_{k_{IL}+1/k_{IL}} = \left[\mathbf{I} + \mathbf{A}_1 + \mathbf{A}_2 + \cdots + \mathbf{A}_{k_{IL}}\right] \cdot \Delta\widetilde{\mathbf{X}}_1 \tag{47}$$

where

$$\mathbf{A}_\eta = C_{k_{IL}}^{\eta} \cdot \left[\frac{\mathbf{F}_0}{f_I}\right]^{\eta}, \eta = 1, \ldots, k_{IL}. \tag{48}$$

The relation of $\mathbf{A}_\eta$ can be further deduced

$$\frac{\mathbf{A}_\eta}{\mathbf{A}_{\eta-1}} = \frac{C_{k_{IL}}^{\eta}}{C_{k_{IL}}^{\eta-1}} \cdot \mathbf{F}_0. \tag{49}$$

Calculate the maximum value of the above formula

$$\max\left(\frac{\mathbf{A}_\eta}{\mathbf{A}_{\eta-1}}\right) = \left(\frac{1}{2f_L} - \frac{1}{2f_I}\right) \cdot \mathbf{F}_0. \tag{50}$$

Therefore, we ignore higher order terms, and the formula is further simplified

$$\Delta\widetilde{\mathbf{X}}_{k_{IL}+1/k_{IL}} \approx \left[\mathbf{I} + C_{k_{IL}}^1 \cdot \frac{\mathbf{F}_0}{f_I}\right] \cdot \Delta\widetilde{\mathbf{X}}_1. \tag{51}$$

Then, the final state error is

$$\Delta\widetilde{\mathbf{X}}_{k_{IL}+1/k_{IL}} \approx \left[\mathbf{I} + \frac{\mathbf{F}_0}{f_L}\right] \cdot \mathbf{K}_1 \cdot \Delta\widetilde{\mathbf{p}}_1^{G,\text{Spoofed}}. \tag{52}$$

According to the specific form of $\mathbf{F}_0$ [30], the elements of $(\mathbf{F}_0/f_L)$ related to the position are much smaller than 1. To facilitate subsequent analysis, we simplify the final state error

$$\Delta\widetilde{\mathbf{X}}_{k_{IL}+1/k_{IL}} \approx \mathbf{K}_1 \cdot \Delta\widetilde{\mathbf{p}}_1^{G,\text{Spoofed}}. \tag{53}$$

From the derivation results, it can be seen that, when the IMU is working normally, the change of positioning error due to the spoofing attack is very small, so the IMU has little effect on the results of the positioning error through the state update between the two LiDAR measurement values. This result is consistent with the conclusion in [9], but it does not prove it in theory. Therefore, this article has verified this conclusion theoretically.

C. Error Analysis of LiDAR Measurement Update Process

The subsequent position measurement is LiDAR at epoch k_{IL}. As the covariance matrix of state estimation remains unchanged, the filter gain matrix $\mathbf{K}_{k_{IL}+1}^{L}$ value remains unchanged in the measurement update process of LiDAR position, and the measurement update equation can be expressed as

$$\widetilde{\mathbf{X}}_{k_{IL}+1} = \widetilde{\mathbf{X}}_{k_{IL}+1/k_{IL}} + \mathbf{K}_{k_{IL}+1}^{L}\left(\mathbf{Z}_{k_{IL}} - \mathbf{H}_L\widetilde{\mathbf{X}}_{k_{IL}+1/k_{IL}}\right). \tag{54}$$

Theoretically, when there is no GNSS spoofing attack, the measurement update result is

$$\hat{\mathbf{X}}_{k_{IL}+1} = \hat{\mathbf{X}}_{k_{IL}+1/k_{IL}} + \mathbf{K}_{k_{IL}+1}^{L}\left(\mathbf{Z}_{k_{IL}} - \mathbf{H}_L\hat{\mathbf{X}}_{k_{IL}+1/k_{IL}}\right). \tag{55}$$

The difference of state update results $\Delta\widetilde{\mathbf{X}}_{k_{IL}+1/k_{IL}}$ before and after the spoofing attack can be expressed

$$\Delta\widetilde{\mathbf{X}}_{k_{IL}+1/k_{IL}} = \widetilde{\mathbf{X}}_{k_{IL}+1/k_{IL}} - \hat{\mathbf{X}}_{k_{IL}+1/k_{IL}}. \tag{56}$$

Thus, the state update results at epoch $k_{IL}+1$ can be obtained

$$\Delta\widetilde{\mathbf{X}}_{k_{IL}+1} \approx \left(\mathbf{I} - \mathbf{K}_{k_{IL}+1}^{L}\mathbf{H}_L\right)\Delta\widetilde{\mathbf{X}}_1 \tag{57}$$

where

$$\mathbf{K}_{k_{IL}+1}^{L} = \mathbf{P}_{k_{IL}+1/k_{IL}}\mathbf{H}_L^T\left(\mathbf{H}_L\mathbf{P}_{k_{IL}+1/k_{IL}}\mathbf{H}_L^T + \mathbf{R}_L\right)^{-1} \tag{58}$$

where $\mathbf{R}_L$ is the measurement noise covariance matrix that describes the uncertainty of LiDAR measurement values. From the above formula, when the position result of the LiDAR is still correct, the correction capability of the positioning error caused by GNSS spoofing is mainly related to the filter gain matrix of LiDAR. The filter gain matrix is mainly related to the state covariance matrix and the measurement noise matrix at this epoch

$$\Delta\widetilde{\mathbf{X}}_{k_{IL}+1} \approx \left(\mathbf{I} - \mathbf{K}_{k_{IL}+1}^{L}\mathbf{H}_L\right)\mathbf{K}_1^G \cdot \Delta\widetilde{\mathbf{p}}_1^{G,\text{Spoofed}}. \tag{59}$$

After the measurement update process of LiDAR, the state propagation process is re-entered until the MSF system receives the next LiDAR epoch, and then, the measurement update is performed. Due to the low GNSS update frequency, the cycle is repeated before the next GNSS epoch is received, and there are k_{LG} cycles.

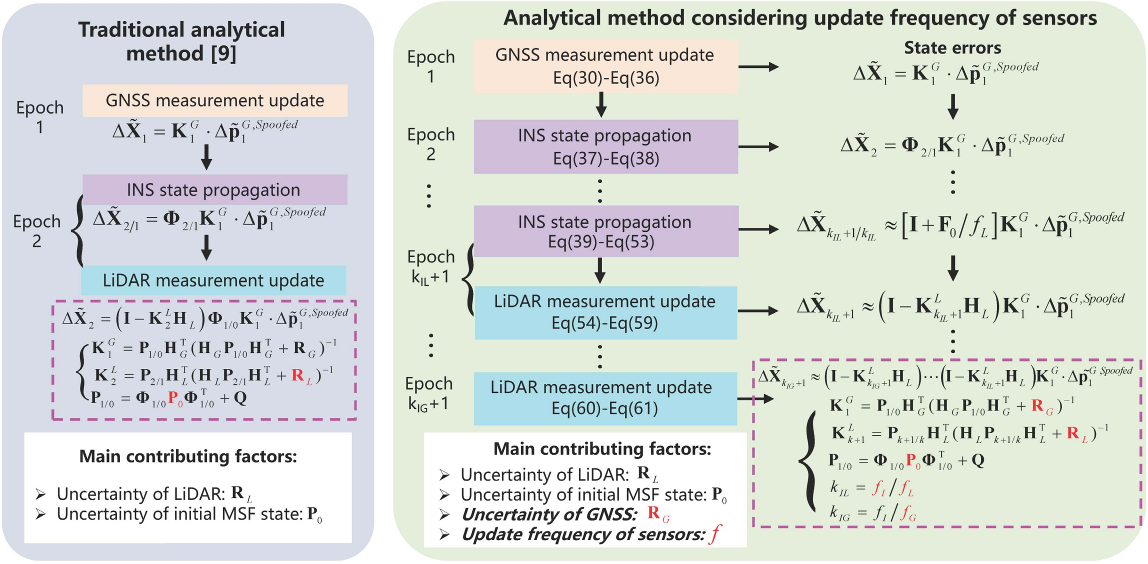

Traditional analytical method [9]
Epoch 1
GNSS measurement update
$\Delta\tilde{\mathbf{X}}_1 = \mathbf{K}_1^G \cdot \Delta\tilde{\mathbf{p}}_1^{G,Spoofed}$
Epoch 2
INS state propagation
$\Delta\tilde{\mathbf{X}}_{2/1} = \mathbf{\Phi}_{2/1}\mathbf{K}_1^G \cdot \Delta\tilde{\mathbf{p}}_1^{G,Spoofed}$
LiDAR measurement update
$\Delta\tilde{\mathbf{X}}_2 = \left(\mathbf{I} - \mathbf{K}_2^L\mathbf{H}_L\right)\mathbf{\Phi}_{1/0}\mathbf{K}_1^G \cdot \Delta\tilde{\mathbf{p}}_1^{G,Spoofed}$
$\mathbf{K}_1^G = \mathbf{P}_{1/0}\mathbf{H}_G^T(\mathbf{H}_G\mathbf{P}_{1/0}\mathbf{H}_G^T + \mathbf{R}_G)^{-1}$
$\mathbf{K}_2^L = \mathbf{P}_{2/1}\mathbf{H}_L^T(\mathbf{H}_L\mathbf{P}_{2/1}\mathbf{H}_L^T + \mathbf{R}_L)^{-1}$
$\mathbf{P}_{1/0} = \mathbf{\Phi}_{1/0}\mathbf{P}_0\mathbf{\Phi}_{1/0}^T + \mathbf{Q}$
Main contributing factors:
➢ Uncertainty of LiDAR: $\mathbf{R}_L$
➢ Uncertainty of initial MSF state: $\mathbf{P}_0$
Analytical method considering update frequency of sensors
Epoch 1
GNSS measurement update Eq(30)-Eq(36)
Epoch 2
INS state propagation Eq(37)-Eq(38)
INS state propagation Eq(39)-Eq(53)
Epoch k_{IL}+1
LiDAR measurement update Eq(54)-Eq(59)
Epoch k_{IG}+1
LiDAR measurement update Eq(60)-Eq(61)
State errors
$\Delta\tilde{\mathbf{X}}_1 = \mathbf{K}_1^G \cdot \Delta\tilde{\mathbf{p}}_1^{G,Spoofed}$
$\Delta\tilde{\mathbf{X}}_2 = \mathbf{\Phi}_{2/1}\mathbf{K}_1^G \cdot \Delta\tilde{\mathbf{p}}_1^{G,Spoofed}$
$\Delta\tilde{\mathbf{X}}_{k_{IL}+1/k_{IL}} \approx \left[\mathbf{I} + \mathbf{F}_0/f_L\right]\mathbf{K}_1^G \cdot \Delta\tilde{\mathbf{p}}_1^{G,Spoofed}$
$\Delta\tilde{\mathbf{X}}_{k_{IL}+1} \approx \left(\mathbf{I} - \mathbf{K}_{k_{IL}+1}^L\mathbf{H}_L\right)\mathbf{K}_1^G \cdot \Delta\tilde{\mathbf{p}}_1^{G,Spoofed}$
$\Delta\tilde{\mathbf{X}}_{k_{IG}+1} \approx \left(\mathbf{I} - \mathbf{K}_{k_{IG}+1}^L\mathbf{H}_L\right)\cdots\left(\mathbf{I} - \mathbf{K}_{k_{IL}+1}^L\mathbf{H}_L\right)\mathbf{K}_1^G \cdot \Delta\tilde{\mathbf{p}}_1^{G\ Spoofed}$
$\mathbf{K}_1^G = \mathbf{P}_{1/0}\mathbf{H}_G^T(\mathbf{H}_G\mathbf{P}_{1/0}\mathbf{H}_G^T + \mathbf{R}_G)^{-1}$
$\mathbf{K}_{k+1}^L = \mathbf{P}_{k+1/k}\mathbf{H}_L^T(\mathbf{H}_L\mathbf{P}_{k+1/k}\mathbf{H}_L^T + \mathbf{R}_L)^{-1}$
$\mathbf{P}_{1/0} = \mathbf{\Phi}_{1/0}\mathbf{P}_0\mathbf{\Phi}_{1/0}^T + \mathbf{Q}$
$k_{IL} = f_I/f_L$
$k_{IG} = f_I/f_G$
Main contributing factors:
➢ Uncertainty of LiDAR: $\mathbf{R}_L$
➢ Uncertainty of initial MSF state: $\mathbf{P}_0$
➢ *Uncertainty of GNSS:* $\mathbf{R}_G$
➢ *Update frequency of sensors:* f

Fig. 5. Comparison between a traditional analytical model [9] and the proposed analytical model considering sensors' update frequency.

There are only the measurement update process of LiDAR and the state propagation process of INS. If the vehicle is relatively stable, the system noise characteristics are unchanged. From epoch 1 to epoch $k_{IG}+1$, we assume that the state noise and measurement noise change little. Therefore, before the next GNSS epoch comes at epoch $k_{IG}+1$, the positioning error caused by the GNSS spoofing can be approximately simplified as follows:

$$\Delta\widetilde{\mathbf{X}}_{k_{IG}+1} \approx \left(\mathbf{I} - \mathbf{K}^L_{k_{IG}+1}\mathbf{H}_L\right)\cdots\left(\mathbf{I} - \mathbf{K}^L_{k_{IL}+2}\mathbf{H}_L\right) \cdot \left(\mathbf{I} - \mathbf{K}^L_{k_{IL}+1}\mathbf{H}_L\right)\mathbf{K}^G_1 \cdot \Delta\widetilde{\mathbf{p}}_1^{G,\text{Spoofed}} \tag{60}$$

where

$$\mathbf{K}^G_1 = \mathbf{P}_{1/0}\mathbf{H}_G^T\left(\mathbf{H}_G\mathbf{P}_{1/0}\mathbf{H}_G^T + \mathbf{R}_G\right)^{-1} \tag{61a}$$

$$\mathbf{K}^L_{k+1} = \mathbf{P}_{k+1/k}\mathbf{H}_L^T\left(\mathbf{H}_L\mathbf{P}_{k+1/k}\mathbf{H}_L^T + \mathbf{R}_L\right)^{-1}. \tag{61b}$$

D. Analysis Comparing to the Existing Analytical Model

In one GNSS spoofing attack cycle, we derive the state propagation process and the measurement update process of the standard KF. To make the analysis clear, we compare the analytical method proposed in this article and the traditional method [9], and summarize the actual filter process and the state error due to the GNSS spoofing attack. The results are shown in Fig. 5.

On the one hand, the state error caused by the GNSS attack is related to the attack intensity $\Delta\widetilde{\mathbf{p}}_1^{G,\text{Spoofed}}$ and attack time T (the next GNSS spoofing attack can be accumulated on the current positioning error, so the final spoofed distance is also related to the time when the attacker can perform GNSS spoofing) of the attacker. On the other hand, for the MSF system, through the traditional analysis method, the state error $\Delta\widetilde{\mathbf{X}}_{k_{IG}+1}$ caused by the attacker is mainly related to LiDAR uncertainty $\mathbf{R}_L$ and initial MSF state uncertainty $\mathbf{P}_0$ in one GNSS spoofing attack cycle [9]. Through the analytical method proposed in this article, the state error $\Delta\widetilde{\mathbf{X}}_{k_{IG}+1}$ caused by the attacker is not only related to the above two factors but also related to GNSS uncertainty $\mathbf{R}_G$ and the sensors' update frequency f.

However, it is still not explicit how the main contributing factors affect the final integrated solution under the spoofing attack. For example, the larger the uncertainty $\mathbf{R}_L$, and uncertainty $\mathbf{R}_G$ means the better immunity against spoofing attack. In addition, how does the different update rate of measurements affect the immunity? To answer these questions, we further derive the analytical model in a form of the information filer to avoid the complex inverse derivation in the KF. Moreover, it should be noted that the analytic model of standard KF considering update frequency under a GNSS spoofing attack is the basis for the following.

IV. Analytic Model of Information Filter Under a GNSS Spoofing Attack

To make the relationship between the positioning error caused by spoofing attack and the factors of $\mathbf{R}_L$, $\mathbf{R}_G$, $\mathbf{P}_0$, and f more explicit, we first ignore the INS state update process in the MSF system. As described in Section III-D, the INS state update process has little impact on positioning error caused by the GNSS spoofing, which has been explained in Section III-B and [9]. Therefore, we ignore this process in the MSF system, and the sequent derivation is given in Section IV-1. Second, in view of the complicated measurement update process in the standard KF, we re-establish an analytical model using an information filter [60], avoiding the complex inverse process in the standard measurement update process, which is introduced in Section IV-B.

A. Error Analysis of GNSS Information Update Process

Similar to Section III-A, we also assume that the LiDAR measurement information has just been updated at epoch 0, and then, a GNSS signal exists at epoch 1. According to the information filter process, the information vector prediction value and the one-step information matrix can be expressed as

$$\mathbf{I}_{1/0}^{-1} = \Phi_{1/0}\mathbf{P}_0\Phi_{1/0}^T + \mathbf{Q} \tag{62a}$$
$$\hat{\mathbf{S}}_{1/0} = \mathbf{I}_{1/0}\hat{\mathbf{X}}_{1/0}. \tag{62b}$$

Then, the information matrix can be expressed as

$$\mathbf{I}_1 = \mathbf{I}_{1/0} + \mathbf{H}_1^T\mathbf{R}_G^{-1}\mathbf{H}_1. \tag{63}$$

The spoofed information vector update equation and the actual information vector update equation are

$$\widetilde{\mathbf{S}}_1 = \hat{\mathbf{S}}_{1/0} + \mathbf{H}_1^T\mathbf{R}_G^{-1}\widetilde{\mathbf{Z}}_1 \tag{64a}$$
$$\hat{\mathbf{S}}_1 = \hat{\mathbf{S}}_{1/0} + \mathbf{H}_1^T\mathbf{R}_G^{-1}\hat{\mathbf{Z}}_1. \tag{64b}$$

As we can see, the information matrix $\hat{\mathbf{S}}_{1/0}$ of the information filter is identical. Then, the information vector error caused by the GNSS spoofing attack can be expressed as

$$\Delta\widetilde{\mathbf{S}}_1 = \mathbf{H}_1^T\mathbf{R}_G^{-1}\Delta\widetilde{\mathbf{Z}}_1 \tag{65}$$

where $\Delta\widetilde{\mathbf{S}}_1 = \mathbf{I}_1\Delta\widetilde{\mathbf{X}}_1$, $\Delta\widetilde{\mathbf{Z}}_1 = \Delta\widetilde{\mathbf{p}}_1^{G,\text{Spoofed}}$, and then, the state error after the GNSS spoofing can be further obtained

$$\Delta\widetilde{\mathbf{X}}_1 = \mathbf{I}_1^{-1}\mathbf{H}_1^T\mathbf{R}_G^{-1}\Delta\widetilde{\mathbf{p}}_1^{G,\text{Spoofed}}. \tag{66}$$

B. Error Analysis of LiDAR Information Update Process

Since the LiDAR update frequency f_L is greater than the GNSS update frequency f_G in general, the following position measurement information is LiDAR at epoch k_{IL}. Based on the above analysis, we ignore the INS status update process in the MSF system, so there is little change in the information vector error and the information matrix

$$\Delta\widetilde{\mathbf{S}}_{k_{IL}+1/k_{IL}} \approx \Delta\widetilde{\mathbf{S}}_1 \tag{67a}$$
$$\mathbf{I}_{k_{IL}+1/k_{IL}} \approx \mathbf{I}_1. \tag{67b}$$

The information update equation can be expressed as

$$\widetilde{\mathbf{S}}_{k_{IL}+1} = \widetilde{\mathbf{S}}_{k_{IL}+1/k_{IL}} + \mathbf{H}_2^T\mathbf{R}_L^{-1}\mathbf{Z}_{k_{IL}+1} \tag{68a}$$
$$\mathbf{I}_{k_{IL}+1} = \mathbf{I}_{k_{IL}+1/k_{IL}} + \mathbf{H}_2^T\mathbf{R}_L^{-1}\mathbf{H}_2. \tag{68b}$$

Theoretically, when there is no GNSS spoofing attack, the information update equation is

$$\hat{\mathbf{S}}_{k_{IL}+1} = \hat{\mathbf{S}}_{k_{IL}+1/k_{IL}} + \mathbf{H}_2^T\mathbf{R}_L^{-1}\mathbf{Z}_{k_{IL}+1}. \tag{69}$$

The difference between the information vector before and after the GNSS spoofing attack can be expressed

$$\Delta\widetilde{\mathbf{S}}_{k_{IL}+1} = \Delta\widetilde{\mathbf{S}}_{k_{IL}+1/k_{IL}}. \tag{70}$$

Because $\Delta\widetilde{\mathbf{S}}_{k_{IL}+1/k_{IL}} \approx \Delta\widetilde{\mathbf{S}}_1$ and $\mathbf{I}_{k_{IL}+1/k_{IL}} \approx \mathbf{I}_1$, the information vector error and the information matrix can be simplified

$$\Delta\widetilde{\mathbf{S}}_{k_{IL}+1} \approx \Delta\widetilde{\mathbf{S}}_1 \tag{71a}$$
$$\mathbf{I}_{k_{IL}+1} \approx \mathbf{I}_1 + \mathbf{H}_2^T\mathbf{R}_L^{-1}\mathbf{H}_2. \tag{71b}$$

Further derivation can be obtained

$$\Delta\widetilde{\mathbf{X}}_{k_{IL}+1} \approx \mathbf{I}_{k+1}^{-1}\mathbf{I}_{k_{IL}+1/k_{IL}}\Delta\widetilde{\mathbf{X}}_{k_{IL}+1/k_{IL}}. \tag{72}$$

Then, the state error can be expressed as

$$\Delta\widetilde{\mathbf{X}}_{k_{IL}+1} \approx \left(\mathbf{I}_1 + \mathbf{H}_2^T\mathbf{R}_L^{-1}\mathbf{H}_2\right)^{-1}\mathbf{H}_1^T\mathbf{R}_G^{-1}\Delta\widetilde{\mathbf{p}}_1^{G,\text{Spoofed}}. \tag{73}$$

From the above formula, when the position results of the LiDAR are still correct, the correction capability of the positioning error caused by GNSS spoofing is mainly related to the filter information matrix at this epoch and the initial information matrix $\mathbf{I}_1$.

Theoretically, after the information update process of LiDAR, the state update process is re-entered until the MSF system receives the next LiDAR epoch, and then, the measurement update is performed. However, we ignore the state update process during this analysis process when the MSF system receives the following LiDAR values at epoch $2k_{IL}+1$. Then, the difference between the information vector error before and after the GNSS spoofing attack can be expressed

$$\Delta\widetilde{\mathbf{S}}_{2k_{IL}+1} = \Delta\widetilde{\mathbf{S}}_{k_{IL}+1/k_{IL}} \tag{74a}$$
$$\mathbf{I}_{2k_{IL}+1} = \mathbf{I}_{k_{IL}+1/k_{IL}} + \mathbf{H}_2^T\mathbf{R}_L^{-1}\mathbf{H}_2 \tag{74b}$$

where $\mathbf{I}_{k_{IL}+1/k_{IL}} \approx \mathbf{I}_{k_{IL}+1}$ and $\Delta\widetilde{\mathbf{S}}_{k_{IL}+1/k_{IL}} \approx \Delta\widetilde{\mathbf{S}}_{k_{IL}+1}$. Then, further derivation can be obtained

$$\Delta\widetilde{\mathbf{S}}_{2k_{IL}+1} \approx \Delta\widetilde{\mathbf{S}}_1 \tag{75a}$$
$$\mathbf{I}_{2k_{IL}+1} \approx \mathbf{I}_1 + 2\cdot\mathbf{H}_2^T\mathbf{R}_L^{-1}\mathbf{H}_2. \tag{75b}$$

The state error can be expressed as

$$\Delta\widetilde{\mathbf{X}}_{2k_{IL}+1} \approx \left(\mathbf{I}_1 + 2\cdot\mathbf{H}_2^T\mathbf{R}_L^{-1}\mathbf{H}_2\right)^{-1}\mathbf{H}_1^T\mathbf{R}_G^{-1}\Delta\widetilde{\mathbf{p}}_1^{G,\text{Spoofed}}. \tag{76}$$

Due to the low GNSS update frequency, the information update process of LiDAR is repeated before the next GNSS epoch is received, and there are k_{LG} cycles. There are only the measurement update process of LiDAR and the state update process of INS. If the vehicle is relatively stable, the system noise characteristics are unchanged. From epoch 1 to epoch $k_{IG}+1$, the state noise and the measurement noise are changed little. Therefore, before the next GNSS epoch comes at epoch $k_{IG}+1$, the information vector error changes little so that it can be approximately simplified as

$$\Delta\widetilde{\mathbf{S}}_{k_{IG}+1} \approx \Delta\widetilde{\mathbf{S}}_1 \tag{77a}$$
$$\mathbf{I}_{k_{IG}+1} \approx \mathbf{I}_1 + k_{LG}\cdot\mathbf{H}_2^T\mathbf{R}_L^{-1}\mathbf{H}_2. \tag{77b}$$

Because $\Delta\widetilde{\mathbf{S}}_1 = \mathbf{H}_1^T\mathbf{R}_G^{-1}\Delta\widetilde{\mathbf{p}}_1^{G,\text{Spoofed}}$ and $\Delta\widetilde{\mathbf{X}}_{k_{IG}+1} = \mathbf{I}_{k_{IG}+1}^{-1}\Delta\widetilde{\mathbf{S}}_1$, then the state error caused by the GNSS spoofing attack can be approximately simplified as

$$\Delta\widetilde{\mathbf{X}}_{k_{IG}+1} \approx \left(\mathbf{I}_1 + k_{LG}\cdot\mathbf{H}_2^T\mathbf{R}_L^{-1}\mathbf{H}_2\right)^{-1}\mathbf{H}_1^T\mathbf{R}_G^{-1}\Delta\widetilde{\mathbf{p}}_1^{G,\text{Spoofed}}. \tag{78}$$

C. Analysis

We summarize the actual filter process and the state errors due to the GNSS spoofing attack, as shown in Fig. 5. By comparing Figs. 5 and 6, although the information filter is essentially the same as the standard KF, it is more intuitive in the expression form of measurement information update.

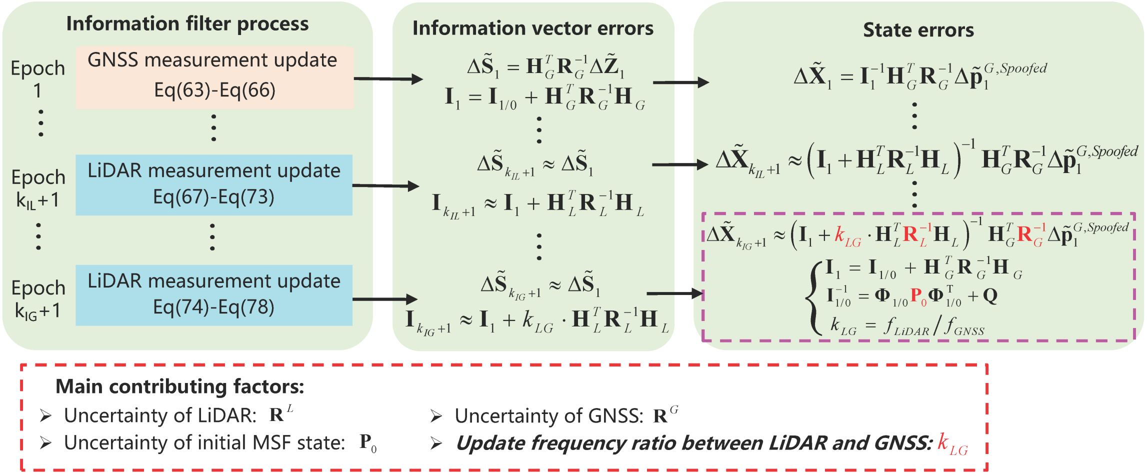

Information filter process
Epoch 1
GNSS measurement update Eq(63)-Eq(66)
Epoch $k_{IL}+1$
LiDAR measurement update Eq(67)-Eq(73)
Epoch $k_{IG}+1$
LiDAR measurement update Eq(74)-Eq(78)
Information vector errors
$\Delta\tilde{\mathbf{S}}_1 = \mathbf{H}_G^T\mathbf{R}_G^{-1}\Delta\tilde{\mathbf{Z}}_1$
$\mathbf{I}_1 = \mathbf{I}_{1/0} + \mathbf{H}_G^T\mathbf{R}_G^{-1}\mathbf{H}_G$
$\Delta\tilde{\mathbf{S}}_{k_{IL}+1} \approx \Delta\tilde{\mathbf{S}}_1$
$\mathbf{I}_{k_{IL}+1} \approx \mathbf{I}_1 + \mathbf{H}_L^T\mathbf{R}_L^{-1}\mathbf{H}_L$
$\Delta\tilde{\mathbf{S}}_{k_{IG}+1} \approx \Delta\tilde{\mathbf{S}}_1$
$\mathbf{I}_{k_{IG}+1} \approx \mathbf{I}_1 + k_{LG}\cdot\mathbf{H}_L^T\mathbf{R}_L^{-1}\mathbf{H}_L$
State errors
$\Delta\tilde{\mathbf{X}}_1 = \mathbf{I}_1^{-1}\mathbf{H}_G^T\mathbf{R}_G^{-1}\Delta\tilde{\mathbf{p}}_1^{G,Spoofed}$
$\Delta\tilde{\mathbf{X}}_{k_{IL}+1} \approx \left(\mathbf{I}_1 + \mathbf{H}_L^T\mathbf{R}_L^{-1}\mathbf{H}_L\right)^{-1}\mathbf{H}_G^T\mathbf{R}_G^{-1}\Delta\tilde{\mathbf{p}}_1^{G,Spoofed}$
$\Delta\tilde{\mathbf{X}}_{k_{IG}+1} \approx \left(\mathbf{I}_1 + k_{LG}\cdot\mathbf{H}_L^T\mathbf{R}_L^{-1}\mathbf{H}_L\right)^{-1}\mathbf{H}_G^T\mathbf{R}_G^{-1}\Delta\tilde{\mathbf{p}}_1^{G,Spoofed}$
$\begin{cases}\mathbf{I}_1 = \mathbf{I}_{1/0} + \mathbf{H}_G^T\mathbf{R}_G^{-1}\mathbf{H}_G \\ \mathbf{I}_{1/0}^{-1} = \mathbf{\Phi}_{1/0}\mathbf{P}_0\mathbf{\Phi}_{1/0}^{\mathrm{T}} + \mathbf{Q} \\ k_{LG} = f_{LiDAR}/f_{GNSS}\end{cases}$
Main contributing factors:
➢ Uncertainty of LiDAR: $\mathbf{R}^L$
➢ Uncertainty of initial MSF state: $\mathbf{P}_0$
➢ Uncertainty of GNSS: $\mathbf{R}^G$
➢ Update frequency ratio between LiDAR and GNSS: k_{LG}

Fig. 6. Information filter update process and state error of the analytical method considering sensors' update frequency.

For the MSF system, through the analytical model based on the information filter, the state error $\Delta\tilde{\mathbf{X}}_{k_{IG}+1}$ caused by the attacker is not only mainly related to LiDAR uncertainty $\mathbf{R}_L$, initial MSF state uncertainty $\mathbf{P}_0$, and GNSS uncertainty $\mathbf{R}_G$ but also related to the update frequency ratio k_{LG} between LiDAR and GNSS. Different from the results obtained by the standard KF process, the form of the state error is obviously simpler by means of the simplified analytical model proposed in this chapter. From the final state error formula due to the GNSS spoofing attack in one GNSS update cycle, we can easily analyze the relationship between these essential parameters and the state error.

1) The state error is positively correlated with $\mathbf{R}_L$ and $\mathbf{P}_0$. That is to say, the smaller $\mathbf{R}_L$ and $\mathbf{P}_0$, the smaller the state error caused by the GNSS spoofing attack.
2) The state error is negatively correlated with $\mathbf{R}_G$ and k_{LG}, which means the larger $\mathbf{R}_G$ and k_{LG}, the smaller the state error caused by the GNSS spoofing attack.

V. Experiment

Since the parameters $\mathbf{R}_L$ and $\mathbf{P}_0$ have been proven to be related to the positioning error under a GNSS spoofing attack in [9], this article focuses on the influence of GNSS uncertainty $\mathbf{R}_G$ and update frequency ratio k_{LG} between LiDAR and GNSS.

A. Setup

The KAIST Complex Urban dataset [61] is selected to verify the theoretical analysis results. The KAIST dataset covers various types of urban scenarios and contains various navigation sensors of different types and accuracies. According to the theoretical analysis results in this article, the data are selected under the following conditions to ensure the success rate of GNSS spoofing attacks.

1) Relatively open scenes with good GNSS signals (low GNSS uncertainty).
2) Relatively limited feature points on both sides of the lane, with medium LiDAR localization accuracy (medium LiDAR uncertainty). If there are no feature points on both sides, LiDAR may not be able to get matching results, which will lead to a complete failure of LiDAR.

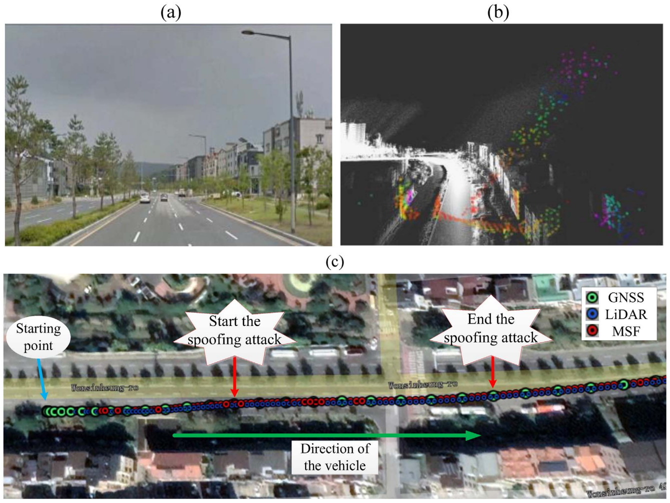


Fig. 7. (a) Real-world view of urban-07 in the KAIST dataset. (b) NDT matching results of Autoware. (c) Dataset positioning results before spoofing attacks based on the GNSS/IMU/LiDAR MSF algorithm.

According to the conditions, the initial phase of the dataset in the KAIST urban-07 is selected for the actual data processing, which has good GNSS signals and limited feature points on both sides of the lane, and the real-world view of this scenario is shown in Fig. 7(a). As the high-precision maps are not provided in the KAIST dataset, this article builds the LiDAR point cloud maps through the localization module in Autoware [62]. The mapping and matching results are shown in Fig. 7(b) using the method of normal-distributions' transform (NDT) [31].

In the dataset of the KAIST urban-07, the vehicle starts from a standstill and runs eastward in the direction of the lane from 5 s. The specifications of the relevant sensors can be found in the literature [61]. In the MSF algorithm, we performed a time alignment between the different navigation sensors and initial attitude alignment, so there is no time and space

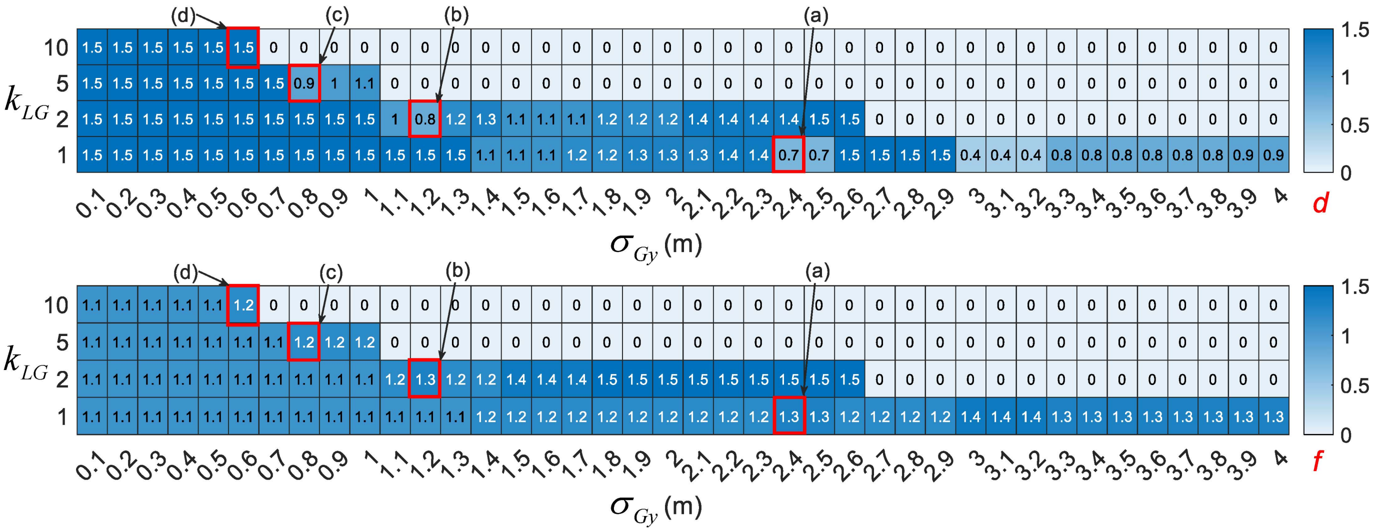


Fig. 8. Optimal spoofing parameters *d* and *f* of a successful attack under different σ_{Gy}'s and k_{LG}'s. (a) GNSS uncertainty and (b) update frequency ratio. Note that the *Y*-axis positioning noise STD σ_{Ly} of LiDAR is set as 2 m because of the medium LiDAR localization accuracy.

asynchronous problem in the result of the MSF system. In particular, the update frequencies of GNSS, LiDAR, and IMU are 5, 10, and 100 Hz, respectively. We can change the update frequency (the update frequency of GNSS is 5 or 1 Hz, and the update frequency of LiDAR is 10 or 5 Hz) by downsampling in order to verify the impact of k_{LG}, which are 1, 2, 5 and 10 through different combinations. In this section, we set the update frequencies of GNSS and LiDAR are changed as 1 and 5 Hz, respectively. Then, the GNSS, LiDAR, and IMU data in the dataset are used to achieve MSF localization via the loosely coupled KF. The final positioning results in the world coordinate system before spoofing attacks are shown in Fig. 7(c).

B. Perform Spoofing Attacks Under Different $\mathbf{R}_G$'s and k_{LG}'s

Under the chi-square test, persistent spoofing attacks are performed. At first, we need to find the optimal spoofing parameters d and f that can maximize the lateral deviation within the attack window. If the parameters are too smaller, the spoofing time will be longer, and if the parameters are too larger, the attack will be easily detected by the MSF system. Therefore, we set d within the range from 0.3 to 1.5 m, and f is changeable from 1.1 to 1.5, which is based on the literature [9]. The optimal parameters will be found by an enumeration method under different $\mathbf{R}_G$'s and k_{LG}'s

$$\mathbf{R}_G = \begin{bmatrix} \sigma_{Gx}^2 & 0 & 0 \\ 0 & \sigma_{Gy}^2 & 0 \\ 0 & 0 & \sigma_{Gz}^2 \end{bmatrix} \tag{79}$$

where σ_{Gx}, σ_{Gy}, and σ_{Gz} are the 3-D positioning noise standard deviations (STDs) of GNSS. We will start a GNSS malicious spoofing attack in the latitude direction (which is the northern direction in this dataset) at the 20 s, so the change of σ_{Gy} represents the change of $\mathbf{R}_G$, then set the spoofing attack window as 10 s, and perform a sustained GNSS spoofing attack using the method of maximizing the lateral deviation, which is introduced in Section II-B. In order to make the simulation conditions consistent, the spoofing value is unchanged in 1 s.

In addition, we follow the fusion ripper to calculate the thresholds, which are generally calculated by vehicle width and lane width [9]. For the vehicle's width, we use the width of the reference car, the Lincoln MKZ [63]. For the lane's width, we refer to the design guidelines [64] published by the U.S. Department of Transportation Federal Highway Administration. Hence, $L = 3.6$ m, and $C = 2.11$ m; then, we can calculate $D_{\text{th-1}}$ and $D_{\text{th-2}}$, which are set to 0.745 and 2.855 m, respectively. When the lateral deviation exceeds $D_{\text{th-1}}$, the constant value attack scheme turns to the exponential value attack scheme. When the lateral deviation exceeds $D_{\text{th-2}}$, the attack is successful. The thresholds will not be frequently triggered in normal conditions due to the high-precious positioning results of the MSF systems.

Fig. 8 shows the optimal spoofing parameters d and f that can be found within the attack window under different $\mathbf{R}_G$'s and k_{LG}'s. The horizontal axis represents σ_{Gy}, which is between 0.1 and 4 m, and the vertical axis represents k_{LG}, which are 1, 2, 5, and 10, respectively. The "0" value means that no parameter can be found to make the maximum lateral deviation exceed 2.855 m, so the MSF system cannot be spoofed successfully in this condition. The blue parts represent the MSF system in dangerous scenes where σ_{Gy} and k_{LG} are smaller, so spoofing parameters can be found to perform successful attacks. The white parts represent the MSF system in safe scenes where σ_{Gy} and k_{LG} are too large at the same time, so no parameter can be found to perform a successful attack in a continuous attack window.

Our purpose is to find the largest spoof parameters d and f, which can cause a larger deviation and a shorter successful time. However, too larger d and f may cause a deviation that exceeds the threshold of the chi-square test, so the spoofed GNSS measurements will be treated as outliers by the MSF system. Therefore, four successful spoofing scenes are selected to study in detail, marked red in Fig. 8. The cases are analyzed how the chi-square test restricts the spoofing attack and also

TABLE I

MAXIMUM LATERAL DEVIATION OF DIFFERENT k_{LG}'S AND σ_{Gy}'S. THE MARKED BOLD ARE THE MAXIMUM LATERAL DEVIATION THAT WE NEED TO FIND THAT CAN BE ACHIEVED AND THE CORRESPONDING COMBINATION OF ATTACK PARAMETERS UNDER THE SAME k_{LG} AND σ_{Gy}

k_{LG} **and** σ_{Gy}	**Maximum Lateral Deviation (m)**	f	d
(a) k_{LG}=1, σ_{Gy}=2.4m	3.58	1.1	1.5
	6.35	1.2	1.4
	6.37	**1.3**	**0.7**
	5.35	1.4	0.3
(b) k_{LG}=2, σ_{Gy}=1.2m	4.60	1.1	1.5
	8.07	1.2	1.1
	8.18	**1.3**	**0.8**
	4.31	1.4	0.7
	8.13	1.5	0.7
(c) k_{LG}=5, σ_{Gy}=0.8m	3.92	1.1	1.5
	10.85	**1.2**	**0.9**
	4.22	1.3	0.5
	0.94	1.4	0.3
	0.94	1.5	0.3
(d) k_{LG}=10, σ_{Gy}=0.6m	2.40	1.1	1.5
	3.18	**1.2**	**1.5**
	3.08	1.3	1.4
	2.56	1.4	1.3
	2.84	1.5	1.3

explains how the well-planned attack scheme performs a successful attack using the vulnerability of the chi-square test. In order to facilitate statistics, in the four cases, we change the parameter f from 1.1 to 1.5 and find the largest d, which can cause the largest lateral deviation, that is, the parameters exceeding the largest d will be detected by the chi-square test. The results are shown in Table I and Fig. 9.

From the results, although LiDAR will correct the positioning results between two GNSS epochs, the deviation will gradually increase with the continuous spoofing attack, but the changes of the horizontal deviations are different in the four cases. It is worth noting the following.

1) We have no statistics when $f = 1.5$ in Fig. 9(a) because all d will be detected by the chi-square test that we cannot perform a successful spoof in this condition, so it is not that the larger the parameters, the better the attack result.
2) Some parameter combinations in Fig. 9(b) and (c) will trigger the take-over effect [9], that is, the correct LiDAR positioning results are regarded as outliers by the chi-square test, which causes the MSF system to completely believe the measurements of the spoofed GNSS, making the positioning results quickly diverged.
3) Fig. 9(d) is a critical scene in which very few results can exceed the threshold. Although we can perform successful attacks, there are very few attack parameters that can be found due to the chi-square test, so it is difficult to perform a successful attack in this scene.

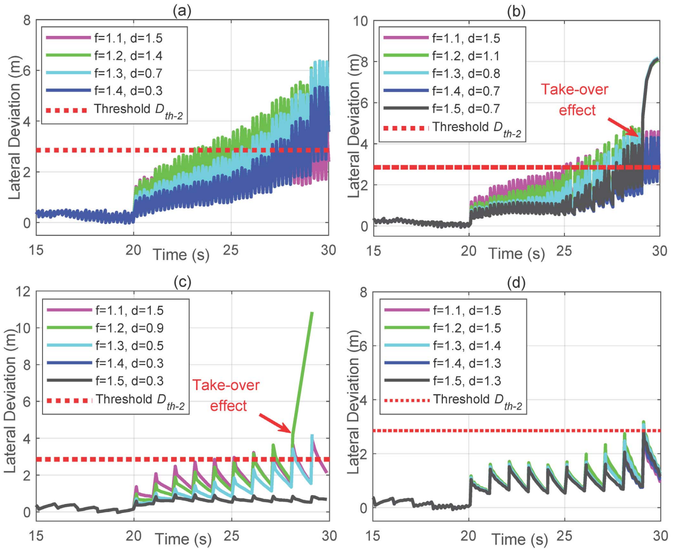


Fig. 9. Lateral deviation of different k_{LG}'s and σ_{Gx}'s under a GNSS spoofing attack within the 10-s attack window. (a) $\sigma_{Gy} = 2.4$ m and $k_{LG} = 1$, where $f_L = 5$ Hz and $f_G = 5$ Hz. (b) $\sigma_{Gy} = 1.2$ m and $k_{LG} = 2$, where $f_L = 10$ Hz and $f_G = 5$ Hz. (c) $\sigma_{Gy} = 0.8$ m and $k_{LG} = 5$, where $f_L = 5$ Hz and $f_G = 1$ Hz. (d) $\sigma_{Gy} = 0.6$ m and $k_{LG} = 10$, where $f_L = 10$ Hz and $f_G = 1$ Hz.

On the one hand, due to the restrictions of the chi-square test, the maximum value of d that can be found will decrease as the increase of f, so the maximum deviation that an attack can achieve will be limited. On the other hand, for some slowly changed spoofing schemes, the positioning errors are gradually increasing, so it is difficult to detect via the chi-square test, which is commonly used in many MSF systems. Worse still, the correct positioning results may be regarded as outliers by the chi-square test, such as the take-over effect, so it provides opportunities for these well-designed attack schemes.

C. Attack Effectiveness Under Different $\mathbf{R}_G$'s and k_{LG}'s

In this section, we mainly verify the attack effectiveness under different $\mathbf{R}_G$'s and k_{LG}'s with the corresponding optimal spoofing parameters d and f from two aspects: the maximum lateral deviation and the minimum time of a successful spoofing attack. The real data processing results are shown in Figs. 10 and 11.

From the results, when k_{LG} is a fixed value, the larger the σ_{Gy}, the smaller the lateral deviations, and the larger the minimum time of a successful spoofing attack, which means the lower the spoofing success rate. This is because, when the GNSS uncertainty is larger, the MSF system trusts it less, and the MSF system trusts the LiDAR measurement values more, so GNSS has less influence on the output of the MSF system. Therefore, the results are consistent with the theoretical analysis in Sections III-D and IV-C.

Similarly, when σ_{Gy} is a fixed value, the larger the k_{LG}, the smaller the lateral deviations, and the larger the minimum time of a successful spoofing attack, which means the lower the spoofing success rate. This is because, when the update frequency of LiDAR is higher than that of GNSS, there are more LiDAR measurement values between two GNSS signals

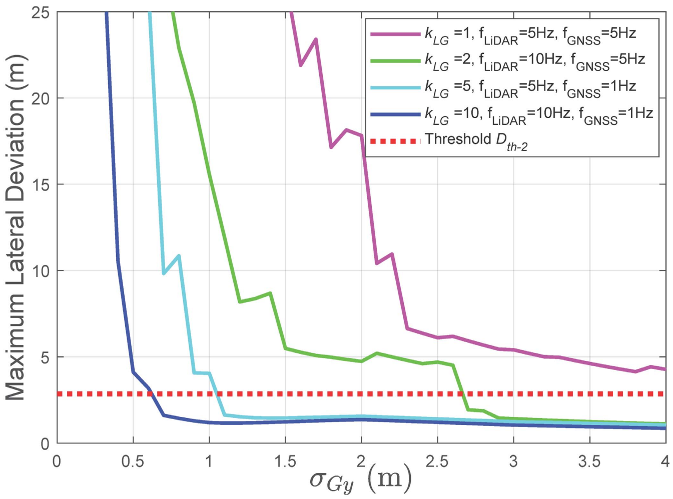


Fig. 10. Maximum lateral deviation under a GNSS spoofing attack.

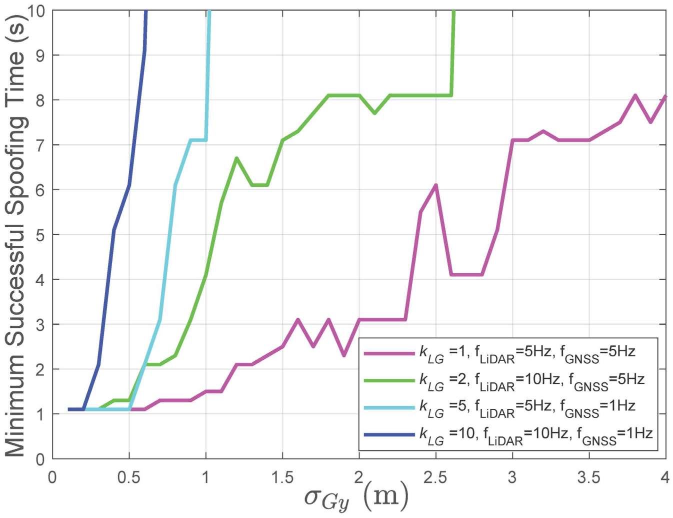


Fig. 11. Minimum successful time for reaching the required deviation of 2.855 m under a GNSS spoofing attack.

to correct the deviation caused by the attack, thus increasing the difficulty of the attack and reducing the probability of a successful spoofing attack. Therefore, the experiment results in this section validate the analyses in Sections III and IV.

VI. Discussion

As we can see in Section V, a successful spoofing attack can cause more than ten meters of lateral deviation within a 10-s attack window. However, the width of the lane line is usually only a few meters, so the position deviation of the MSF system greatly increases the safety risk of the vehicle in the field of automatic driving. Under such elaborate spoofing attacks, the vehicle is likely to be out of the driveway or hit the vehicle on the opposite side, causing severe traffic accidents. In essence, attackers can find some scenes, when the uncertainty of LiDAR is larger, and the uncertainty of GNSS is smaller, and then perform quick attacks to achieve a high spoofing success rate. Therefore, from the perspective of the victim, in order to avoid being successfully spoofed, some schemes can be considered from the following points.

1) Improve the performance and update frequency of LiDAR (decrease $\mathbf{R}_L$ and increase k_{LG}), and maintain vigilance when driving into scenarios and environments where the LiDAR is performing too bad.
2) Improve the KF model (decrease $\mathbf{P}_0$) and the monitoring efficiency of the GNSS spoofing attack (increase $\mathbf{R}_G$).

VII. Conclusion

This article introduces a GNSS spoofing attack scheme and develops an analytical model considering the impact of different sensors' update frequency based on a loosely coupled GNSS/LiDAR/INS KF model. With this model, the error mechanism of GNSS spoofing behavior is analyzed in detail, and the main contributing factors to the positioning error are found, including the uncertainty of the initial MSF state, the uncertainty of LiDAR, the uncertainty of GNSS, and the update frequency of different sensors. Then, the filter model is appropriately simplified by ignoring inconsequential parameters, and the analytical model is re-established using the information filter. We discover that the update frequency ratio between LiDAR and GNSS is also a primary contributing factor related to the positioning error under the spoofing attack. We perform real trace world data experiments to verify the theoretical analysis results. In our experiments, when the update frequency ratio between GNSS and LiDAR is 1, 2, 5, and 10, the STD of GNSS is smaller than 4, 2.7, 1.1, and 0.7 m, respectively, and a successful spoof can be performed within a 10-s attack window. It should be noted that a successful spoofing attack may cause more than 10-m lateral deviations, which may cause severe traffic accidents. Finally, we give suggestions for anti-GNSS spoofing design.

References

[1] R. da Costa, "EUSPA EO and GNSS market report," Eur. Union Agency Space Programme (EUSPA), Prague, Czech Republic, Tech. Rep. 2443-5236, 2022, pp. 11–20.

[2] B. Hofmann-Wellenhof, H. Lichtenegger, and E. Wasle, *GNSS—Global Navigation Satellite Systems: GPS, GLONASS, Galileo, and More*. Vienna, Austria: Springer, 2007.

[3] G. Johnston, A. Riddell, and G. Hausler, "The international GNSS service," in *Springer Handbook of Global Navigation Satellite Systems*. Cham, Switzerland: Springer, 2017, pp. 967–982.

[4] Q. Lu, X. Feng, and C. Zhou, "A detection and weakening method for GNSS time-synchronization attacks," *IEEE Sensors J.*, vol. 21, no. 17, pp. 19069–19077, Sep. 2021.

[5] D. A. Grejner-Brzezinska, C. K. Toth, T. Moore, J. F. Raquet, M. M. Miller, and A. Kealy, "Multisensor navigation systems: A remedy for GNSS vulnerabilities?" *Proc. IEEE*, vol. 104, no. 6, pp. 1339–1353, Jun. 2016.

[6] V. Sreeja, "Impact and mitigation of space weather effects on GNSS receiver performance," *Geosci. Lett.*, vol. 3, no. 1, pp. 1–13, 2016.

[7] E. Falletti, D. Margaria, G. Marucco, B. Motella, M. Nicola, and M. Pini, "Synchronization of critical infrastructures dependent upon GNSS: Current vulnerabilities and protection provided by new signals," *IEEE Syst. J.*, vol. 13, no. 3, pp. 2118–2129, Sep. 2019.

[8] Y. Hu, S. Bian, B. Li, and L. Zhou, "A novel array-based spoofing and jamming suppression method for GNSS receiver," *IEEE Sensors J.*, vol. 18, no. 7, pp. 2952–2958, Apr. 2018.

[9] J. Shen, J. Y. Won, Z. Chen, and Q. A. Chen, "Drift with devil: Security of multi-sensor fusion based localization in high-level autonomous driving under GPS spoofing," in *Proc. 29th USENIX Secur. Symp.*, Boston, MA, USA, Aug. 2020, pp. 931–948.

[10] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Capkun, "On the requirements for successful GPS spoofing attacks," in *Proc. 18th ACM Conf. Comput. Commun. Secur.*, 2011, pp. 75–86.

[11] J. R. van der Merwe, X. Zubizarreta, I. Lukčin, A. Rügamer, and W. Felber, "Classification of spoofing attack types," in *Proc. Eur. Navigat. Conf. (ENC)*, May 2018, pp. 91–99.

[12] P. D. Groves, "Principles of GNSS, inertial, and multisensor integrated navigation systems," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 30, no. 2, pp. 26–27, Mar. 2015.

[13] G. Wan et al., "Robust and precise vehicle localization based on multisensor fusion in diverse city scenes," in *Proc. IEEE Int. Conf. Robot. Autom. (ICRA)*, May 2018, pp. 4670–4677.

[14] 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, no. 4, pp. 1–31, May 2016.

[15] W. Farag, "Real-time autonomous vehicle localization based on particle and unscented Kalman filters," *J. Control, Autom. Electr. Syst.*, vol. 32, no. 2, pp. 309–325, 2021.

[16] D. Huang, H. Leung, and N. El-Sheimy, "Expectation maximization based GPS/INS integration for land-vehicle navigation," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 43, no. 3, pp. 1168–1177, Jul. 2007.

[17] Y. Fang, H. Min, W. Wang, Z. Xu, and X. Zhao, "A fault detection and diagnosis system for autonomous vehicles based on hybrid approaches," *IEEE Sensors J.*, vol. 20, no. 16, pp. 9359–9371, Aug. 2020.

[18] W. Wen, X. Bai, Y. Kan, and L. Hsu, "Tightly coupled GNSS/INS integration via factor graph and aided by fish-eye camera," *IEEE Trans. Veh. Technol.*, vol. 68, no. 11, pp. 10651–10662, Nov. 2019.

[19] L. Chang, X. Niu, T. Liu, J. Tang, and C. Qian, "GNSS/INS/LiDAR-SLAM integrated navigation system based on graph optimization," *Remote Sens.*, vol. 11, no. 9, p. 1009, 2019.

[20] W. Wen, T. Pfeifer, X. Bai, and L. T. Hsu, "Factor graph optimization for GNSS/INS integration: A comparison with the extended Kalman filter," *J. Inst. Navigat.*, vol. 68, no. 2, pp. 315–331, 2020.

[21] Q. Meng and L.-T. Hsu, "Integrity monitoring for all-source navigation enhanced by Kalman filter-based solution separation," *IEEE Sensors J.*, vol. 21, no. 14, pp. 15469–15484, Jul. 2021.

[22] C. Sanders and Y. Wang, "Localizing spoofing attacks on vehicular GPS using vehicle-to-vehicle communications," *IEEE Trans. Veh. Technol.*, vol. 69, no. 12, pp. 15656–15667, Dec. 2020.

[23] J. S. Gipson and R. C. Leishman, "Resilience for multi-filter all-source navigation framework with integrity," in *Proc. IEEE 24th Int. Conf. Inf. Fusion*, Sun City, South Africa, 2021.

[24] J. D. Jurado and J. F. Raquet, "Autonomous and resilient management of all-source sensors," in *Proc. I_{ON} Pacific PNT Meeting*, 2019, pp. 142–159.

[25] G. Johnson, P. Swaszek, J. Alberding, M. Hoppe, and J.-H. Oltmann, "The feasibility of R-mode to meet resilient PNT requirements for e-navigation," in *Proc. 27th Int. Tech. Meeting Satell. Division Inst. Navigat.*, 2014, pp. 3076–3100.

[26] Y. Yuanxi, "Resilient PNT concept frame," *Acta Geodaetica Cartographica Sinica*, vol. 47, no. 7, p. 893, 2018.

[27] G. Zhang and L.-T. Hsu, "Intelligent GNSS/INS integrated navigation system for a commercial UAV flight control system," *Aerosp. Sci. Technol.*, vol. 80, pp. 368–380, Sep. 2018.

[28] X. Gao et al., "RL-AKF: An adaptive Kalman filter navigation algorithm based on reinforcement learning for ground vehicles," *Remote Sens.*, vol. 12, no. 11, p. 1704, 2020.

[29] Y. Zhang, L. Wang, N. Qiao, X. Tang, and B. Li, "A low-cost GPS/INS integration methodology based on DGPM during GPS outages," in *Proc. Integr. Commun., Navigat., Surveill. Conf. (ICNS)*, Apr. 2018, pp. 4E2-1–4E2-8.

[30] Y. Gongmin and Y. Deng, "Review on practical Kalman filtering techniques in traditional integrated navigation system," *Navigat. Position. Timing*, vol. 7, no. 2, pp. 50–64, 2020.

[31] N. Akai et al., "Autonomous driving based on accurate localization using multilayer LiDAR and dead reckoning," in *Proc. IEEE 20th Int. Conf. Intell. Transp. Syst. (ITSC)*, Oct. 2017, pp. 1–6.

[32] Y. Qin, H. Zhang, and S. Wang, *Principles of Kalman Filter and Integrated Navigation*. Xi'an, China: Northwestern Polytechnical Univ. Press, 2015.

[33] B. Pardhasaradhi and P. Srihari, "Stealthy GPS spoofer design by incorporating processing time and clock offsets," in *Proc. IEEE 18th India Council Int. Conf. (INDICON)*, Dec. 2021, pp. 1–6.

[34] E. Schmidt, J. Lee, N. Gatsis, and D. Akopian, "Rejection of smooth GPS time synchronization attacks via sparse techniques," *IEEE Sensors J.*, vol. 21, no. 1, pp. 776–789, Jan. 2020.

[35] P. Bethi, S. Pathipati, and P. Aparna, "GNSS intentional interference mitigation via average KF innovation and pseudo track updation," in *Proc. IEEE 17th India Council Int. Conf. (INDICON)*, Dec. 2020, pp. 1–5.

[36] J. Zidan, E. I. Adegoke, E. Kampert, S. A. Birrell, C. R. Ford, and M. D. Higgins, "GNSS vulnerabilities and existing solutions: A review of the literature," *IEEE Access*, vol. 9, pp. 153960–153976, 2020.

[37] L. Xiao, P.-C. Ma, X.-M. Tang, and G.-F. Sun, "GNSS receiver anti-spoofing techniques: A review and future prospects," in *Electronics, Communications and Networks V*. Singapore: Springer, 2016, pp. 59–68.

[38] P. Bethi, S. Pathipati, and P. Aparna, "Impact of target tracking module in GPS spoofer design for stealthy GPS spoofing," in *Proc. IEEE 17th India Council Int. Conf. (INDICON)*, Dec. 2020, pp. 1–6.

[39] B. Pardhasaradhi and L. R. Cenkeramaddi, "GPS spoofing detection and mitigation for drones using distributed radar tracking and fusion," *IEEE Sensors J.*, vol. 22, no. 11, pp. 11122–11134, Jun. 2022.

[40] Z. Wu, Y. Zhang, Y. Yang, C. Liang, and R. Liu, "Spoofing and anti-spoofing technologies of global navigation satellite system: A survey," *IEEE Access*, vol. 8, pp. 165444–165496, 2020.

[41] E. Schmidt, Z. Ruble, D. Akopian, and D. J. Pack, "Software-defined radio GNSS instrumentation for spoofing mitigation: A review and a case study," *IEEE Trans. Instrum. Meas.*, vol. 68, no. 8, pp. 2768–2784, Aug. 2019.

[42] Y. Liu, S. Li, Q. Fu, Z. Liu, and Q. Zhou, "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, Aug. 2019.

[43] L. Zhang, H. Zhao, C. Sun, L. Bai, and W. Feng, "Enhanced GNSS spoofing detector via multiple-epoch inertial navigation sensor prediction in a tightly-coupled system," *IEEE Sensors J.*, vol. 22, no. 9, pp. 8633–8647, May 2022.

[44] Ç. Tanil, S. Khanafseh, M. Joerger, and B. Pervan, "An INS monitor to detect GNSS spoofers capable of tracking vehicle position," *IEEE Trans. Aerosp. Electron Syst.*, vol. 54, no. 1, pp. 131–143, Feb. 2018.

[45] Y. Wei, H. Li, and M. Lu, "A steady-state spoofing detection and exclusion method based on raw IMU measurement," *IEEE Sensors J.*, vol. 22, no. 4, pp. 3529–3539, Feb. 2022.

[46] Q. Zhang, X. Niu, and C. Shi, "Impact assessment of various IMU error sources on the relative accuracy of the GNSS/INS systems," *IEEE Sensors J.*, vol. 20, no. 9, pp. 5026–5038, May 2020.

[47] Y. Qin, H. Zhang, and S. Wang, *Kalman Filter and Integrated Navigation Principle*. Evanston, IL, USA: Northwest Industry Univ. Publishing Company, 1998.

[48] G. Yan, J. Wang, and X. Zhou, "High-precision simulator for strapdown inertial navigation systems based on real dynamics from GNSS and IMU integration," in *Proc. China Satell. Navigat. Conf. (CSNC)*. Berlin, Germany: Springer, 2015, pp. 789–799.

[49] G. Yan and J. Weng, *Strapdown Inertial Navigation Algorithm and Principles of Integrated Navigation*. Xi'an, China: Northwestern Polytechnical Univ. Press, 2019.

[50] G. Yan, S. Li, and Y. Qin, *Inertial Instrument Testing and Data Analysis*. Beijing, China: National Defense Industry Publishing, 2012.

[51] G. Yan, C. Zhao, F. Wu, and Y.-Y. Qin, "An improvement for the calibration of laser gyro strapdown IMU," in *Proc. 32nd Chin. Control Conf.*, Jul. 2013, pp. 4861–4865.

[52] G. Yan, X. Yang, X. Su, J. Weng, and Y. Qin, "Error distribution method and analysis of observability degree based on the covariances in Kalman filter," in *Proc. 37th Chin. Control Conf. (CCC)*, Jul. 2018, pp. 4900–4905.

[53] G. Yan, X. Sun, J. Weng, Q. Zhou, and Y. Qin, "Time-asynchrony identification between inertial sensors in SIMU," *J. Syst. Eng. Electron.*, vol. 26, no. 2, pp. 346–352, 2015.

[54] J. Kelly and G. S. Sukhatme, "Visual-inertial sensor fusion: Localization, mapping and sensor-to-sensor self-calibration," *Int. J. Robot. Res.*, vol. 30, no. 1, pp. 56–79, 2011.

[55] M. Schreiber, H. Königshof, A.-M. Hellmund, and C. Stiller, "Vehicle localization with tightly coupled GNSS and visual odometry," in *Proc. IEEE Intell. Vehicles Symp. (IV)*, Jun. 2016, pp. 858–863.

[56] R. Piché, "Online tests of Kalman filter consistency," *Int. J. Adapt. Control Signal Process.*, vol. 30, no. 1, pp. 115–124, 2016.

[57] N. A. Heckert et al., *Handbook 151: NIST/SEMATECH E-Handbook of Statistical Methods*. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2002.

[58] X. Liu, Y. Ju, X. Liu, S. Miao, and W. Zhang, "An IMU fault diagnosis and information reconstruction method based on analytical redundancy for autonomous underwater vehicle," *IEEE Sensors J.*, vol. 22, no. 12, pp. 12127–12138, Jun. 2022.

[59] P. Bethi, S. Pathipati, and P. Aparna, “Stealthy GPS spoofing: Spoofer systems, spoofing techniques and strategies,” in *Proc. IEEE 17th India Council Int. Conf. (INDICON)*, Dec. 2020, pp. 1–7.

[60] N. Assimakis, M. Adam, and A. Douladiris, “Information filter and Kalman filter comparison: Selection of the faster filter,” *Int. J. Inf. Eng.*, vol. 2, no. 1, pp. 1–5, 2012.

[61] J. Jeong, Y. Cho, Y.-S. Shin, H. Roh, and A. Kim, “Complex urban dataset with multi-level sensors from highly diverse urban environments,” *Int. J. Robot. Res.*, vol. 38, no. 6, pp. 642–657, May 2019.

[62] S. Kato et al., “Autoware on board: Enabling autonomous vehicles with embedded systems,” in *Proc. ACM/IEEE 9th Int. Conf. Cyber-Phys. Syst. (ICCPS)*, Apr. 2018, pp. 287–296.

[63] (2019). *2019 MKZ*. [Online]. Available: https://www.lincoln.com/

[64] W. J. Stein and T. R. Neuman, “Mitigation strategies for design exceptions,” Federal Highway Administration, Washington, DC, USA, Tech. Rep. FHWA-SA-07-011, 2007.

Jiachong Chang received the B.S. degree from the Department of Automation, Harbin Engineering University, Harbin, China, in 2016, and the M.S. degree from the School of Instrumentation Science and Engineering, Harbin Institute of Technology, Harbin, in 2018. He is pursuing the Ph.D. degree with the School of Instrumentation Science and Engineering, Harbin Institute of Technology, and the Department of Aeronautical and Aviation Engineering, The Hong Kong Polytechnic University, Hong Kong.

His current research interests include multisensors’ fusion, fault diagnosis technology, and global navigation satellite system (GNSS) spoofing attacks.

Liang Zhang (Member, IEEE) received the Ph.D. degree in instruments science and technology from Southeast University, Nanjing, China, in 2021, and the M.S. degree in navigation, guidance, and control from the Nanjing University of Aeronautics and Astronautics, Nanjing, in 2017.

He is currently a Postdoctoral Fellow with the Interdisciplinary Division of Aeronautical and Aviation Engineering (AAE), The Hong Kong Polytechnic University, Hong Kong. His research interests include inertial navigation, integrated navigation technology, and underwater positioning technology.

Li-Ta Hsu (Senior Member, IEEE) received the B.S. and Ph.D. degrees in aeronautics and astronautics from National Cheng Kung University, Tainan, Taiwan, in 2007 and 2013, respectively.

He was a Postdoctoral Researcher with the Institute of Industrial Science, The University of Tokyo, Tokyo, Japan. In 2012, he was a Visiting Scholar with University College London, London, U.K. He is currently an Associate Professor with the Department of Aeronautical and Aviation Engineering, The Hong Kong Polytechnic University, Hong Kong. His research interests include global navigation satellite system (GNSS) positioning in challenging environments and localization for pedestrians, autonomous driving vehicles, and unmanned aerial vehicles.

Bing Xu (Member, IEEE) received the B.Eng. and Ph.D. degrees from the Nanjing University of Science and Technology, Nanjing, China, in 2012 and 2018, respectively.

He was a Postdoctoral Fellow with The Hong Kong Polytechnic University, Hong Kong, where he is currently a Research Assistant Professor with the Department of Aeronautical and Aviation Engineering. His research focuses on signal processing with applications to positioning systems and wireless communications.

Feng Huang (Graduate Student Member, IEEE) received the bachelor’s degree in automation from Shenzhen University, Shenzhen, China, in 2014, and the M.Sc. degree in electronic engineering from The Hong Kong University of Science and Technology, Hong Kong, in 2016. He is pursuing the Ph.D. degree with the Department of Aeronautical and Aviation Engineering, The Hong Kong Polytechnic University, Hong Kong.

His research interests include localization and sensor fusion for autonomous driving.

Dingjie Xu received the B.S., M.S., and Ph.D. degrees from the Harbin Institute of Technology, Harbin, China, in 1988, 1991, and 1998, respectively.

He is a Professor and a Doctoral Tutor with the School of Instrumentation Science and Engineering, Harbin Institute of Technology. His current research interests include high-precision navigation algorithms, satellite navigation, and robust filtering algorithms.