Selection of Areas for Effective GNSS Spoofing Attacks to a Vehicle-mounted MSF System based on Scenario Classification Models

Jiachong Chang*, Feng Huang, Liang Zhang*, Dingjie Xu, Li-Ta Hsu

***Abstract*—The inherent vulnerability of the Global Navigation Satellite System (GNSS) leads to the ease of implementation of spoofing attacks. The latest GNSS spoofing attack schemes still suffer from low success rate, long attack time, and poor concealment. To improve the success rate, an efficient GNSS spoofing attack method for a vehicle-mounted Multi Sensors Fusion (MSF) system is proposed based on the scenario classification models with a spatial database. Firstly, the influence of the two typical urban scenarios, which are 1) the road with buildings on both sides and 2) tunnels, on the GNSS spoofing attack is analyzed. Then a dynamic Bayesian network model considering the sky visibility generated with the 3D building models and tunnel models inside the spatial database is established to quantify the difficulty of the attack. Furthermore, the scenarios of the victim can be classified into high-risk and low-risk scenarios. When the vehicle is just out of the tunnel or in open scenarios, attackers can select these high-risk scenarios and implement aggressive spoofing attacks. Then the efficiency of the GNSS spoofing attack can be significantly improved. Finally, the proposed attack scheme is demonstrated by actual world data with simulated spoofing attacks in urban areas.**

***Index Terms*—GNSS spoofing attacks, vehicle-mounted MSF navigation system, 3D building models, tunnel, Bayesian network**

I. Introduction

AUTONOMOUS driving technology has rapidly been improved and has become an essential development in the next generation of vehicle technology [1][2]. Autonomous Vehicles (AVs) are required to provide centimeter-level positioning accuracy for safe navigation [3][4]. However, the current localization technology is not mature in response to various malicious spoofing attack methods, including Global Navigation Satellite System (GNSS) spoofing methods [5][6], Light Detection and Ranging (LiDAR) spoofing methods [7][8], camera spoofing methods [9][10], Inertial Measurement Unit (IMU) spoofing methods [11][12], etc. These security issues may cause serious traffic accidents and potential risks to the autonomous driving industry [13][14]. Among them, the methods of the GNSS spoofing attack are common [15][16], easily implemented [17], and low cost [18]. Thus, it is one of the most critical safety issues of localization and has attracted widespread attention.

GNSS is a powerful navigational tool, but it is not absolutely secure. The US Department of Transportation first raises concerns about Global Position System (GPS) vulnerabilities and the over-reliance on GPS for critical safety applications [19], which may cause serious consequences. In a simple demonstration performed in a track [20], the GPS receivers are spoofed into reporting false position information every time in simulation, indicating the GPS is vulnerable to spoofing. Over the past decade, GNSS spoofing attacks have been reported in different application areas, such as marine traffic [21], unmanned vehicles [22], aircraft [23], mobile devices [24], etc.

Currently, most researches focus on studying the design of spoofing and defense algorithm in the GNSS/Inertial Navigation System (INS) integrated navigation system, which has been widely used in actual applications [25][26]. Attackers can inject fault information into the GNSS measurements in the tightly coupled GNSS/INS system [27][28]. Some models can detect spoofing by comparing the relative trajectory estimated by the GNSS receiver and high-precision IMU [29][30]. A closed-loop evaluation model is designed to evaluate the impact of GNSS faults on the aircraft with an INS monitor [31]. Covert GNSS spoofing algorithms are performed based on a GPS/INS integrated system in the application of unmanned aerial vehicles [32][33]. The attackers can build a graph model for a given road network and then perform aggressive action to enable them to derive potential destinations [34]. In summary, all of these researches are based on the GNSS/INS integrated navigation system. Due to the lack of position information of a critical observation quantity from LiDAR, the position information output of the GNSS/IMU integrated navigation system will be highly dependent on GNSS. However, many Multi-Sensors Fusion (MSF) systems equip with LiDAR in AVs [35], so these spoofing models may be inefficacy.

Manuscript received xxxx, xxxx; revised xxxx, xxxx; accepted xxxx, xxxx. This research is supported by the University Grants Committee of Hong Kong under the scheme Research Impact Fund on the project R5009-21 "Reliable Multiagent Collaborative Global Navigation Satellite System Positioning for Intelligent Transportation Systems".

(*Corresponding author: Jiachong Chang, Liang Zhang.*). Jiachong Chang is with the School of Instrumentation Science and Engineering, Harbin Institute of Technology, Harbin, China, and also the Department of Aeronautical and Aviation Engineering, Hong Kong Polytechnic University, Hong Kong (e-mail: jiachong.chang@connect.polyu.hk). Feng Huang and Li-Ta Hsu are with the Department of Aeronautical and Aviation Engineering, Hong Kong Polytechnic University, Hong Kong (e-mail: darren-f.huang@connect.polyu.hk, lt.hsu@polyu.edu.hk). Liang Zhang is with the School of Instrument Science and Engineering, the Key Laboratory of Micro-Inertial Instrument and Advanced Navigation Technology, Ministry of Education, Southeast University, Nanjing 210096, China. (e-mail: liangzhang@seu.edu.cn). Dingjie Xu is with the School of Instrumentation Science and Engineering, Harbin Institute of Technology, Harbin, China (e-mail: xdj1966@hit.edu.cn).

In the research on GNSS spoofing attacks for MSF systems, researchers from the University of California, Irvine (UCI) perform the first security study on MSF systems under GPS spoofing and design the Fusion-ripper in vehicle-mounted MSF navigation systems [36]. A spoofing method is proposed in [37], which fools the LiDAR perception module via adversarial trajectory perturbation of GNSS spoofing attack. Furthermore, different attack models are explored and discussed in the robotic vehicle system, and different spoofing attack vectors are discovered, including the aggressive spoofing attack method to MSF [38]. The research on the GNSS spoofing of the Kalman Filter (KF) based on the MSF positioning system for AVs starts late. There are few related research papers to explore the boundaries of spoofing in MSF positioning systems, which may threaten the security of the vehicle-mounted MSF navigation system in the future. Therefore, the research on GNSS spoofing attacks for the MSF model has practical application value.

Since AVs inevitably operate in various complex and dynamic scenarios, do the latest spoofing attack schemes cover all application scenarios? In what scenarios can a spoofing attack be more likely to succeed? What kind of models can evaluate the vulnerability of GNSS? There have been few papers discussing the above issues. Therefore, this paper conducts the first research on the above problems, aiming to fill the gaps in related fields. We focus on the environment in which MSF systems are more likely to spoof and propose a novel spoofing attack algorithm based on scenario classification models. Aiming at the MSF navigation system of AVs based on a loosely-coupled KF, this paper researches the state-of-the-art GNSS spoofing attack method [36] and explores the boundary of GNSS spoofing technology, and develops a novel GNSS spoofing attack scheme based on scenario classification models. This paper can be summarized from three perspectives. Firstly, we introduce the state-of-the-art spoofing scheme and its problems. Following this, we design and develop scenario classification models to select the high-risk spoofing areas. Finally, we verify our model with real-world data with simulated spoofing attacks, and the efficiency of the GNSS spoofing attack can be significantly improved.

The main contributions of this paper are as follows.

1) The GNSS skyplots are generated through the 3D building models, which eventually generate a sky visibility map. Based on the latest spoofing attack algorithm [36], we establish the link between sky visibility and the uncertainties of LiDAR and GNSS, respectively.

2) We analyze the influence of tunnels on the GNSS spoofing attack. The vulnerability of MSF is demonstrated in this scenario. As a result, attackers can successfully implement efficient GNSS spoofing attacks when the vehicle is just out of the tunnel.

3) We identified urban areas with high GNSS spoofing risks via a Bayesian network model, which can select specific high-risk scenarios with high MSF system vulnerability based on scenario classification models. The model can help attackers improve the efficiency of the GNSS spoofing attack.

The structure of the paper is as follows. Section I is the introduction and includes the current research status. Section II introduces the principle and challenges of the state-of-the-art GNSS spoofing attack scheme for the vehicle-mounted MSF navigation system. Section III illustrates the structure and the parameters of the proposed GNSS spoofing attack method. Section IV establishes the proposed scenario classification models for this effective spoofing attack. Section V verifies the effectiveness of the proposed spoofing attack algorithm through real-world data. Section VI presents the conclusion.

II. Problem Statement

A. Principle of the State-of-the-art GNSS Spoofing Attack Scheme for MSF System

Since most MSF systems are anti-interference, they could prevent temporary outliers or accidental failures. The most common anti-interference method is the Chi-square test, which is widely used in actual applications [39][40]. However, well-designed GNSS spoofing attack schemes can fully use the MSF systems' inherent defects to perform aggressive spoofing attacks. Hence, these advanced GNSS spoofing attack signals are difficult to be detected by defensive measures. An illustration of a state-of-the-art GNSS spoofing attack scheme is shown in Fig.1 [36].

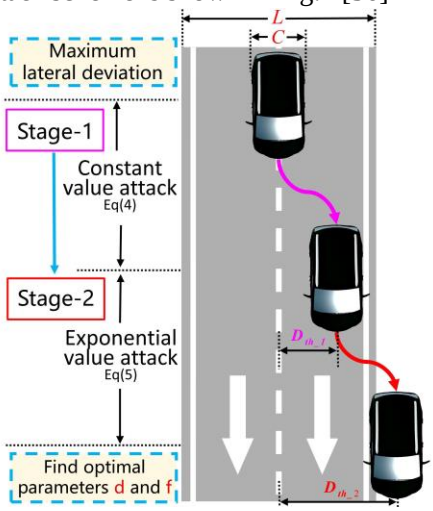


Fig.1. A state-of-the-art GNSS spoofing attack scheme. The principle is to maximize the lateral deviation of the vehicle, and the purpose is to find the spoofing parameters d (the constant value attack parameter) and f (the exponential value attack parameter). Moreover, the two thresholds (D_{th-1} and D_{th-2}) can be calculated via the lane line's width L and the vehicle's width C [36][41].

The maximum GNSS spoofing epoch (k_{max}^{Spoof}) that the attackers can implement is:

$$k_{max}^{Spoof} = T_{max}^{Spoof} \cdot f_G \tag{1}$$

where f_G is the GNSS update frequency, and $T_{max}^{Spoofed}$ is the maximum attack time. Generally, the GNSS spoofing behavior is added a deviation $\Delta\tilde{\boldsymbol{p}}_j^{G\_Spoofed}$ to the real GNSS signal. Hence, the spoofed GNSS sequence can be expressed as:

$$\{\Delta\tilde{\boldsymbol{p}}_1^{G\_Spoofed}, \Delta\tilde{\boldsymbol{p}}_2^{G\_Spoofed}, \cdots, \Delta\tilde{\boldsymbol{p}}_j^{G\_Spoofed}\}, j \le k_{max}^{Spoof} \tag{2}$$

Then the GNSS measurement values can be expressed as:

$$\widetilde{\boldsymbol{p}}_j^G = \boldsymbol{p}_j^G + \Delta\widetilde{\boldsymbol{p}}_j^{G\_Spoofed}, j = 1,2,\cdots and\ j \le k_{max}^{Spoof} \quad (3)$$

where $\widetilde{\boldsymbol{p}}_j^G$ is the spoofed position information, and $\boldsymbol{p}_j^G$ is the original GNSS position information. $\Delta\widetilde{\boldsymbol{p}}_j^{G\_Spoofed} = \begin{bmatrix}\Delta\tilde{L}_j & \Delta\tilde{\lambda}_j & 0\end{bmatrix}^T$ is the deviation. Assume that $\Delta\widetilde{\boldsymbol{X}}_j(p) = \begin{bmatrix}\Delta\widetilde{\boldsymbol{X}}_j^x(p) & \Delta\widetilde{\boldsymbol{X}}_j^y(p) & 0\end{bmatrix}^T$ is the output deviation of the MSF system due to the spoofing attack, where $\Delta\widetilde{\boldsymbol{X}}_j^x(p)$ is the lateral deviation expected to be generated after the spoofing attack and $\Delta\widetilde{\boldsymbol{X}}_j^y(p)$ is the vertical deviation.

The fundamental condition of the scheme is that the deviations cannot be detected by the Chi-square test, and the spoofing time cannot be unlimited. Furthermore, the state-of-the-art spoofing attack scheme is divided into two stages: the constant value spoofing attack scheme and the exponential value spoofing attack scheme.

Stage 1: The purpose of this stage is to find the vulnerable period of the MSF system. In this stage, the parameters and conditions are:

$$\begin{gathered} d = \left\|\boldsymbol{C}_n^b \cdot \Delta\widetilde{\boldsymbol{p}}_j^{G\_Spoofed}\right\| \\ st.1, \left\|\Delta\widetilde{\boldsymbol{X}}_j^x(p)\right\| < D_{th-1} \\ st.2, \chi_j^2 < \chi_{Threshold}^2 \\ st.3, j \le k_{max}^{Spoof} \end{gathered} \quad (4)$$

where d is the attack parameter. $\boldsymbol{C}_n^b$ is the direction cosine matrix from n-frame to b-frame. $\|\cdot\|$ is the process of modular arithmetic. D_{th-1} is the threshold of stage 1. χ_j^2 is the j-th Chi-square test value, and $\chi_{Threshold}^2$ is the threshold of the Chi-square test value. j is the total attack epoch, which is related to the total time for spoofing, k_{max}^{Spoof} the maximum attack epoch due to the limited spoofing time. When the lateral deviation exceeds D_{th-1}, the spoofing attack will enter stage 2, which is an exponential value attack scheme.

Stage 2: When the vulnerability period is found, attackers will perform exponential value spoofing attacks, triggering the take-over effect [36] and quickly completing the spoofing process. The parameters and conditions are:

$$\begin{gathered} d \cdot f^{\tau} = \left\|\boldsymbol{C}_n^b \cdot \Delta\widetilde{\boldsymbol{p}}_j^{G Spoofed}\right\| \\ st.1, D_{th-1} \le \left\|\Delta\widetilde{\boldsymbol{X}}_j^x(p)\right\| < D_{th-2} \\ st.2, \chi_j^2 < \chi_{Threshold}^2 \\ st.3, j \le k_{max}^{Spoof} \end{gathered} \quad (5)$$

where f is the exponential value parameter of the attacker. τ is the exponential value attack epoch. When the lateral deviation exceeds the threshold D_{th-2}, the spoofing attacks are successful.

$$\left\|\Delta\widetilde{\boldsymbol{X}}_j^x(p)\right\| \ge D_{th-2} \quad (6)$$

The principle of this scheme is to maximize the lateral deviation of the vehicle and find the corresponding parameters d and f.

$$\{d, f\} = \mathcal{M}\left\{\Delta\widetilde{\boldsymbol{X}}_j^x(p)\right\} \quad (7)$$

where $\mathcal{M}\{\cdot\}$ is the calculative process to find the parameters d and f via maximizing the lateral deviation.

B. Challenges of the State-of-the-art GNSS Spoofing Attack Scheme for MSF System

1) Despite the difficulty of implementing a successful spoofing attack in some scenarios with poor GNSS quality and high LiDAR signal quality, the state-of-the-art persistent spoofing attack scheme always tries to perform attacks all the time. Therefore, the success rate of aimless multiple attempted attacks is low.

2) The defense measures in many AVs may be strengthened with the development of anti-spoofing technology. Therefore, some new defense algorithms may discover the persistent spoofing attack signals due to the long tracking time.

3) The total time for spoofing is limited. Therefore, the state-of-the-art attack technique may be unable to complete the whole spoofing process in a limited time.

In conclusion, since vehicle-mounted MSF navigation systems inevitably operate in various complex and dynamic scenarios, the state-of-the-art GNSS spoofing attack scheme neglects to consider the impact of environments, so it is inefficient and may be easy to be detected.

III. Parameters and Structure of the Proposed Effective GNSS Spoofing Attack Method

The MSF system can achieve complementary advantages between different sensors, achieving high-precious and robust positioning results in various scenarios, which is an excellent advantage of the MSF system. However, it also provides an opportunity for GNSS spoofing attacks. GNSS and LiDAR signal quality are different in different scenarios [42], so attackers can fully use some specific scenarios where the LiDAR positioning accuracy is not high. In contrast, the GNSS signal quality is better. Our main contribution is to build a more efficient GNSS spoofing attack method with the scenario classification models, improving the success rate and reducing the attack times.

A. Definition of the Spoofing Parameters

Our research object is mainly the AVs, so we mainly analyze the accuracy of navigation sensors in urban environments. For the GNSS positioning accuracy, attackers can judge the received signals' strength and other information to determine the GNSS signal quality of the victim [43]. For the LiDAR positioning accuracy, attackers can confirm the signal quality by judging whether the environmental characteristics around the victim are apparent, such as how many buildings are around the vehicle and whether the peripheral feature points are sufficiently obvious, etc. [44]. Hence, attackers could actively choose to carry out GNSS spoofing attacks in these specific scenes where the LiDAR positioning accuracy is not high. In contrast, the GNSS signals are usually relatively healthy, including some open environments such as elevated roads, suburban roads, roundabouts, highways, and other similar scenarios, as shown in Fig.2. These scenarios can be identified as high-risk areas.

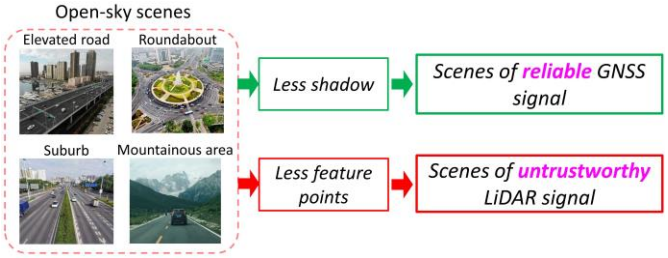


Fig. 2. Scenes of untrustworthy LiDAR signal and reliable GNSS signal.

To facilitate the quantification, we define a few spoofing-related parameters and random variables of the proposed spoofing models. Symbols and their description are shown in Table I.

TABLE I
SYMBOLS AND THEIR DESCRIPTION

Symbol	Description
$\tilde{\boldsymbol{p}}_k$	The position information of the deceived vehicle detected by the attacker. $\tilde{\boldsymbol{p}}_k = [\tilde{L}_k \quad \tilde{\lambda}_k \quad \tilde{h}_k]^T$
$\tilde{\boldsymbol{v}}_k$	The velocity information of the deceived vehicle detected by the attacker. $\tilde{\boldsymbol{v}}_k = [\tilde{v}_k^x \quad \tilde{v}_k^y \quad \tilde{v}_k^z]^T$
M_k	The prior map information.
S_k	The building shadow on both sides of the lane of the spoofed vehicle detected by the attacker. The detailed explanations and demonstrations are in Section IV.C. $S_k = Shadow(\tilde{\boldsymbol{p}}_k) \in (0,1)$
T_k	Whether the vehicle detected by the attacker is running in the tunnel. $T_k = Tunnel(\tilde{\boldsymbol{p}}_k) \in \{yes, no\}$
TO_k	Whether the vehicle detected by the attacker is just out of the tunnel. $TO_k = Tunnel\_Out(\tilde{\boldsymbol{p}}_k) \in \{yes, no\}$
$\tilde{R}_k^G$	The GNSS uncertainty of the spoofed vehicle assessed by the attacker. $\tilde{R}_k^G = Uncertainty\_GNSS(\tilde{\boldsymbol{p}}_k)$
$\tilde{R}_k^L$	The LiDAR uncertainty of the spoofed vehicle assessed by the attacker. $\tilde{R}_k^L = Uncertainty\_LiDAR(\tilde{\boldsymbol{p}}_k)$
A_k	Whether the attacker starts GNSS spoofing attacks on the vehicle. $A_k = Attack(\tilde{\boldsymbol{p}}_k) \in \{yes, no\}$
P_k^A	The probability that the attacker starts GNSS spoofing attacks on the vehicle. $P_k^A = probability(A_k = 1) \in \{1,0\}$

where, M_k denotes the prior map information, including the tunnel information M_k^T, which is a positioning collection about all the tunnels in an area i.g., $\{\boldsymbol{p}_1^T, \boldsymbol{p}_2^T, \cdots, \boldsymbol{p}_i^T\}$. M_k^B denotes the building model information, which is a 3D city building model information in an area. It is defined as follows.

$$M_k = Map(\tilde{\boldsymbol{p}}_k) = \{M_k^B, M_k^T\} \tag{8}$$

B. Structure the Proposed Spoofing Attack Method

To facilitate the quantification of the spoofing attack model, we follow the assumptions of [36] for the attackers and the victims. Moreover, we make some other reasonable assumptions that are theoretically implementable.

For the attackers:

1) Equipped with high-precision navigation sensors and know the actual position and velocity of the victim.

2) Have the ability to perceive the environment of the victim's vehicle and know the tunnel and 3D building model information in which the victim is located.

3) Have the ability to perform a GNSS spoofing attack and completely replace the original GNSS signals of the victim.

For the victims:

1) The victim's MSF system sensors include GNSS, IMU, and LiDAR.

2) The MSF models are based on error-state KF.

3) The uncertainties of GNSS and LiDAR are based on the sensors' quality in different scenarios.

Following these assumptions, attackers can monitor the victim's position and velocity and design scenario classification models to determine whether the victim is in a high-risk spoofing area, as shown in Fig.3.

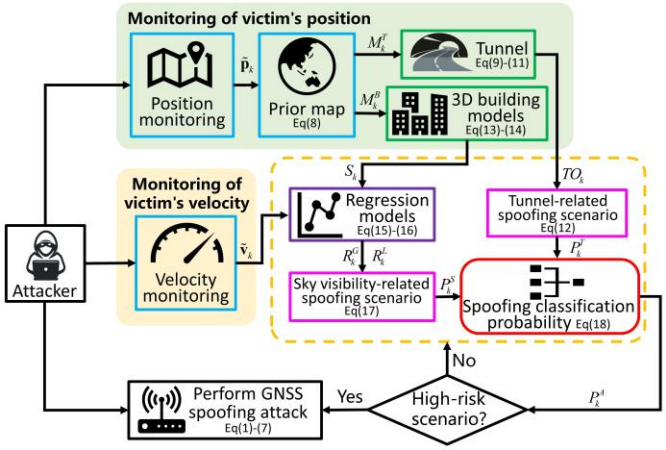


Fig.3. Diagram of the proposed GNSS spoofing attack scheme based on scenario classification models. Blue denotes the prior information of the deceived vehicle detected by attackers. Green denotes the map information of the victim. Purple denotes the regression models. Pink denotes whether it is a high-risk scenario. Red denotes the final spoofing scenarios probability.

It should be noted that this Section mainly introduces the spoofing parameter definition and the structure of the proposed spoofing attack method, so it is the basis for the following sections.

IV. SELECTION OF AREAS FOR EFFECTIVE GNSS SPOOFING ATTACKS BASED ON SCENARIO CLASSIFICATION MODELS

A. Selection of Spoofing Scenarios Related to the Tunnel

Tunnels are common and significant in transport systems, especially in some megacities. Take Hong Kong as an example. There are currently at least 18 tunnels (Over 0.5km) [45] and about 50 corridors [46]. They play an essential role in the movement of passengers and freight. Partial tunnels in Hong Kong are labeled blue on Google earth in Fig.4(A).

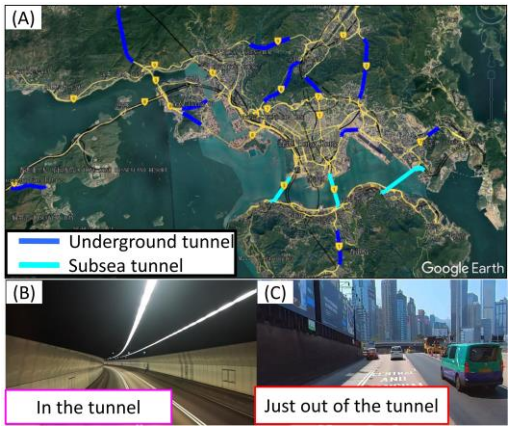


Fig.4. (A) shows the tunnels in Hong Kong [48]. (B) and (C) are real-world scenes when the vehicle is driving in and out of the tunnel, respectively.

Since LiDAR has few effective feature points due to the single feature point in the tunnel, it will cause severe degradation in matching results [47], which has a high chance of leading to longitudinal positioning errors. In addition, the system is in a wholly occluded scenario and will not receive any GNSS information in the tunnel. Therefore, in this scenario, attackers will not conduct spoofing attacks to prevent ineffective attacks. Fig.4(B) shows real-world scenes when the vehicle is driving in the tunnel.

When the vehicle is driving just out of the tunnel, as shown in Fig.4(C), the vehicle can immediately receive the GNSS signals. However, the initial value of the LiDAR signal has a significant error due to the accumulated errors inside the tunnel. The inaccurate initial value will cause the uncertainty of LiDAR to increase rapidly [49]. As a result, the MSF system heavily relies on the GNSS positioning results when the vehicle has just exited the tunnel. Due to the high dependence of the MSF system on GNSS at this point, capturing such a scenario for an effective spoofing attack will significantly increase the success rate, reduce the number of attempts, and decrease the attack time correspondingly. The classification model of the tunnel scenario is established as follows.

At first, the attackers use the monitored position information and prior map information to determine whether the detected vehicle has entered the tunnel, which is defined as follows.

$$P\{T_k = yes|\tilde{\boldsymbol{p}}_k, M_k\} = \begin{cases} 1, (\tilde{L}_k, \tilde{\lambda}_k) \in M_k^T \\ 0, otherwise \end{cases} \quad (9)$$

$$P\{T_k = no|\tilde{\boldsymbol{p}}_k, M_k\} = 1 - P\{T_k = yes|\tilde{\boldsymbol{p}}_k, M_k\} \quad (10)$$

When $P\{T_k = yes\} = 1$, indicating the vehicle has entered the tunnel. After following the vehicle for a while, attackers will determine whether the vehicle has just exited the tunnel or not. The parameters are defined as follows.

$$P\{TO_k = yes|\tilde{\boldsymbol{p}}_k, M_k, T_k\} = \begin{cases} 1, T_k = no, \{\tilde{\boldsymbol{p}}_{k_0-\tau} \cdots \tilde{\boldsymbol{p}}_{k_0-1}\} \in M^T \text{ and } k - k_0 < \kappa \\ 0, otherwise \end{cases} \quad (11)$$

where k_0 is the first point where the vehicle is out of the tunnel. τ is the first point where the vehicle is in the tunnel. κ is the maximum spoofing time when the vehicle is out of the tunnel. Some conditions must be fulfilled when the vehicle has just exited the tunnel.

1) $\{\tilde{\boldsymbol{p}}_{k_0-\tau} \cdots \tilde{\boldsymbol{p}}_{k_0-1}\} \in M^T$, i.e., the vehicle has just been in the tunnel for a while.

2) $P\{T_k = no|\tilde{\boldsymbol{p}}_k, M_k\}$=1, i.e., the vehicle is no longer in the tunnel.

3) $k - k_0 < \kappa$, i.e., the positioning results of LiDAR have not yet fully converged to accurate values evaluated by the MSF system.

Then, attackers determine whether the vehicle is just out of the tunnel with the following equation.

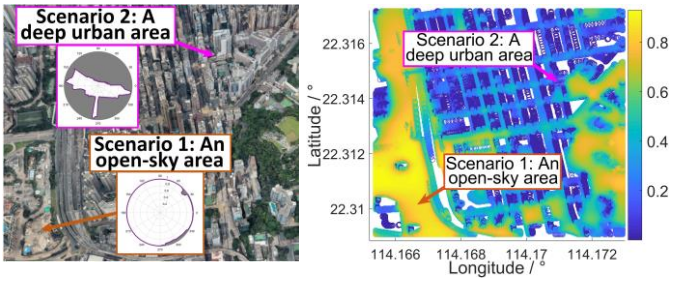
$$P_k^T = \{A_k = yes|TO_k\} = \begin{cases} 1, TO_k = yes \\ 0, otherwise \end{cases} \quad (12)$$

When $P_k^T = 1$, it is a high-risk scenario, indicating the vehicle is just out of the tunnel. Then attackers will capture this specified scenario and quickly perform aggressive GNSS spoofing attacks on the victim.

B. Selection of Spoofing Scenarios Related to the Sky Visibility

The surrounding buildings' number and height directly affect the signal quality of LiDAR and GNSS. Generally, when high buildings are on the sides of the road, the GNSS signal quality will worsen. In this case, the number of visible satellites is reduced due to the building shadow [49]. In addition, the notorious multipath effect may arise, reducing the GNSS positioning accuracy significantly. Conversely, the more buildings on both sides, the more effective feature points can be extracted by the LiDAR theoretically. Furthermore, the LiDAR localization accuracy is higher [44]. Likewise, the GNSS signals are trustworthy when there are few buildings on both sides in some scenarios. In contrast, insufficient effective LiDAR feature points may lead to lower positioning accuracy or even fail to match successfully.

The sky visibility can evaluate the obstruction of the vehicle by buildings on both sides of the road [50]. It is a valuable tool for processing GNSS data, which can reveal the impact of obstructions on satellite visibility. At present, skyplots can be generated via 3D models [51], LiDAR [52], cameras [53], etc. Inspired by these previous works, the attackers can generate a skyplot with the 3D models of the surrounding buildings to evaluate the shadow degree because attackers cannot obtain the LiDAR and GNSS data of the vehicle. Fig.5(A) shows two scenarios' skyplots in Mong Kok of Hong Kong: an open-sky area (Scenario 1) with few buildings and a deep urban area (Scenario 2) with some high facilities on both sides of the road, which are common in modern cities.



(A) (B)

Fig.5. Sky visibility of two real-world scenarios: an open-sky area and

a deep urban area.

We use the ratio of the buildings' shaded area to evaluate the degree of shading, which can be defined as sky visibility.

$$S_k = Shy\_visibility(\tilde{\boldsymbol{p}}_k) = \frac{Area(shadow)}{\pi} \tag{13}$$

$$S_k \in (0,1) \tag{14}$$

where, S_k is the area ratio, which is between 0 and 1, and it indicates the sky visibility in the position $\tilde{\boldsymbol{p}}_k$. $Area(\cdot)$ is to calculate the area of the gray shadow area, as shown in Fig.5(A). When the ratio is higher, the degree of the shadow is lower, and vice versa. When the value is equal to 1, it indicates there are no buildings around the area, and it is an entirely open scene. Then we calculate all the ratios to get the sky visibility of the entire area in Fig.5(A), and the results are shown in Fig.5(B). The yellow regions represent open-sky areas, and the blue regions represent deep urban areas.

It is noted that in some open-sky scenarios, the GNSS signal is trustworthy, and the LiDAR signal quality is poor. Then the system mainly relies on the navigation information provided by GNSS, so the MSF system may be vulnerable to being attacked successfully. We can get the high-risk attack interval via the state-of-the-art spoofing attack algorithm [36]. For instance, when the sampling frequencies of GNSS, LiDAR, and IMU are 1Hz, 10Hz, and 400Hz, respectively, the state-of-the-art spoofing attack scheme is performed to a loosely-couple GNSS/IMU/LiDAR KF MSF system [36][41]. Consequently, Fig.6 indicates the relationship between GNSS and LiDAR uncertainty for a successful spoofing attack. σ_G and σ_L are the standard deviations of GNSS and LiDAR, which are the square root of GNSS uncertainty R_k^G and LiDAR uncertainty R_k^L.

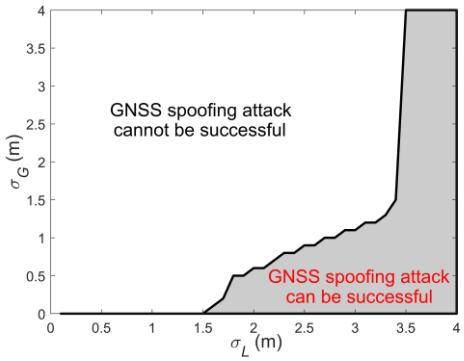


Fig.6. The relationship between GNSS and LiDAR uncertainty for a successful spoofing attack. The right gray part of the curve is defined as the high-risk attack interval.

Furthermore, we build the relationship between the shy visibility, velocity, and uncertainty of GNSS and LiDAR.

$$R_k^G = f^G(S_k) \tag{15}$$

$$R_k^L = f^L(S_k, \tilde{\boldsymbol{v}}_k) \tag{16}$$

where, R_k^G is related to the sky visibility S_k, and the relationship is f^G. We can represent the relationship f^G with a linear least square function of the influential factor. Similarly, R_k^L is related to the sky visibility S_k and the vehicle's velocity $\tilde{\boldsymbol{v}}_k$ assessed by attackers. The relationship is f^L with a linear function of influential factors. In general, the faster the velocity, the worse the quality of LiDAR [54]. Then we can train real data to get the regression function f^G and f^L. Therefore, when the vehicle does not enter the tunnel, the sky visibility can determine whether the vehicle is in a high-risk attack scenario or not.

$$P_k^S = \{A_k = yes | \tilde{R}_k^L, \tilde{R}_k^G, T_k\} = \begin{cases} 1, (\tilde{R}_k^L, \tilde{R}_k^G) \in \Gamma_{LG}, TO_k = no \\ 0 \quad , otherwise \end{cases} \tag{17}$$

where $\tilde{R}_k^G$ is the GNSS uncertainty of the spoofed vehicle assessed by the attacker with the network, $\widetilde{and}\, R_k^L$ is the LiDAR uncertainty of the spoofed vehicle assessed by the attacker with the network. Γ_{LG} is an assemblage that represents the relationship between GNSS uncertainty and LiDAR uncertainty for a successful spoofing attack. When $P_k^S = 1$, the vehicle is in a relatively open-sky area, a high-risk scenario.

C. Scenario Classification Models based on Dynamic Bayesian Network

We build scenario classification models based on a dynamic Bayesian network, which can evaluate whether the MSF system is in a relatively vulnerable state and determine whether the victim is in a region that is easy to be attacked or not. The dynamic Bayesian network model is based on the relationship of these parameters, which are introduced detailedly in Sections IV.B and IV.C. Fig.7 shows two slices of the dynamic Bayesian network model proposed in this paper.

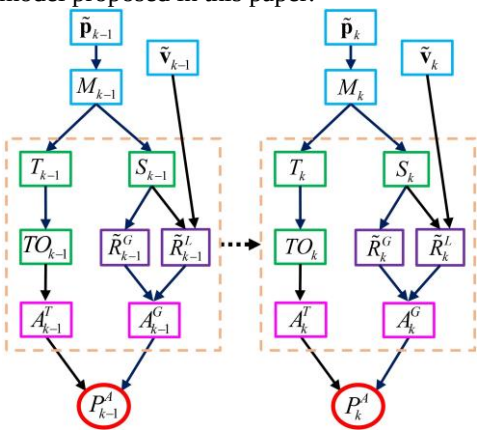


Fig.7. Two slices of the dynamic Bayesian network model. The implications of the colors are the same as in Fig.3. The rectangular and round shapes denote variables and probabilities, respectively.

The output of the network is P_k^A, which is marked red in Fig.7, i.e., the probability that the victim is in a high-risk spoofing scenario. Finally, when $P_k^T = 1$ (Eq.12) or $P_k^S = 1$ (Eq.17), the vehicle is in a high-risk attack scenario, which is related to the tunnel or the sky visibility.

$$P_k^A = \begin{cases} 1, P_k^T = 1 \; or \; P_k^S = 1 \\ 0 \quad , otherwise \end{cases} \tag{18}$$

If $P_k^A = 1$, this scenario is classified as a high-risk attack region for MSF systems, and attackers can capture this specified scenario and quickly perform aggressive GNSS spoofing attacks. Finally, the success rate can be improved significantly.

V. EXPERIMENTS

This paper develops a software platform based on the open-sourcing autonomous driving platform Autoware [55] and the PSINS C++ toolbox [56]. The loosely-couple GNSS/IMU/LiDAR KF MSF algorithm is implemented to further develop and verify the proposed GNSS spoofing attack algorithm. In this Section, some experimental results will be illustrated.

A. Setup

The dataset used is primarily based on the data platform of the Intelligent Positioning and Navigation Laboratory of Hong Kong Polytechnic University [57]. It is an open-sourcing localization dataset collected in Tokyo and Hong Kong. Fig.8 shows the data collection platform and sensors for the Hong Kong dataset. The collection platform is equipped with LiDAR, GNSS, IMU, and other hardware platforms.

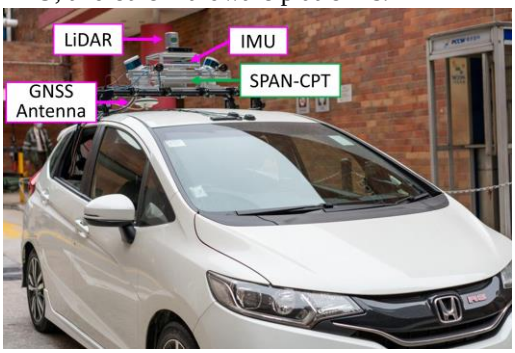


Fig.8. Acquisition platform of Hong Kong dataset. The SPAN-CPT system (green box) can provide ground truth values.

The parameters of the sensors equipped with the data platform are described in Table II:

TABLE II
MAIN SPECIFICATIONS OF THE SENSORS

Sensors	Version	Frequency	Others
3D LiDAR	HDL 32E Velodyne	10Hz	360 HFOV, +10~-30 VFOV, 80m range.
IMU	Xsens Mti 10	400Hz	AHRS
GNSS Receivers	u-blox ZED-F9P	1Hz	GPS L1/L2, Beidou, Galileo.
	NovAtel FlexPak6	1Hz	GPS L1/L2, Beidou, Galileo.
RTK GNSS/INS	NovAtel SPAN-CPT	1Hz	RMSE: 5cm. It provides ground truth values.

In the experiments, we use RTKLIB to obtain the final positioning solution of GNSS [58]. The 'Positioning Model' is set to 'Kinematic'. The 'Integer Ambiguity Resolution' is set to 'Fix and Hold'. The 'Min Ratio to Fix Ambiguity' is 3. Besides, the reference station is about 7km [59].

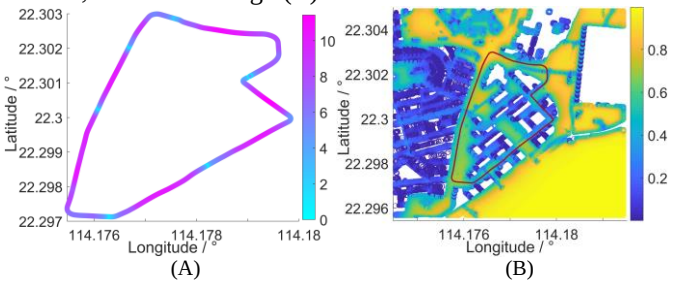
B. GNSS spoofing attack experiment in urban areas

According to the state-of-the-art GNSS attack scheme [36][41], GNSS spoofing attacks are performed on the loosely-couple GNSS/IMU/LiDAR KF MSF system, and the uncertainty estimation of the sensors is based on the signal quality [60][61]. In the spoofing attack experiment, the attack window is set to 10s. We follow the Fusion-ripper to calculate the thresholds of a successful attack, which are generally calculated by the width of the vehicle and lane. Then we calculate the D_{th-1} and D_{th-2} which are set to 0.745m and 2.855m, respectively. When the maximum lateral deviation exceeds 2.855m, it is considered a successful spoofing attack [36][41]. Then we implement GNSS spoofing attacks in two different urban scenarios.

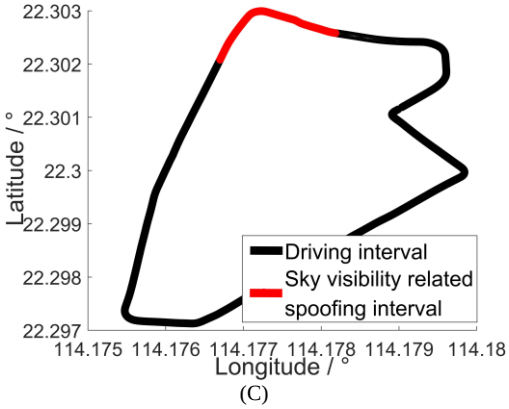
Our research object is based on the GNSS/INS/LiDAR MSF system of AVs. The indicator of the effective evaluation of a GNSS spoofing attack is mainly the 2D positioning error. This parameter determines whether the victim exceeds the threshold or not, and then we can get the spoofing successful number and success rate which directly threatens the system security. Since it is difficult to reflect the spoofing results from other parameters, we only show the most critical results to highlight the main contributions of the proposed model.

Scenario 1:

The first scenario is collected in a typical urban canyon of Hong Kong near Tsim Sha Tsui, which involves high-rising buildings and numerous dynamic objects. In this scenario, the vehicles mainly operate in deep urban areas, simultaneously obscured by tall buildings on both sides, resulting in poor GNSS performance. In addition, there are also some relatively open-sky areas, and the vehicle does not pass through a tunnel. The trajectory and velocity information of the vehicle and the sky visibility information of this area are shown in Fig.9(A) and Fig.9(B). Afterward, the scenario classification model proposed in section IV is used to determine the final high-risk spoofing interval, as shown in Fig.9(C).



(A) (B)



(C)

Fig.9. (A) and (B) are the velocity and sky visibility information of the vehicle. (C) is vehicle trajectory and high-risk attack interval for scenario 1. The red interval is the high-risk area, and the black trajectory is the area unfavorable to attack.

In the manuscript, we fully compare different strategies under the same experimental conditions. Based on previous

research, the main GNSS attack strategies can be divided into the following types: constant value attack, exponential value attack, Fusion-ripper, and the spoofing attack scheme based on the scenario classification model proposed in this paper.

We randomly choose the starting point for the spoofing attack in the high-risk interval and the whole interval. In the experiment, we use two types of GNSS receivers and set the total attack number as 50. As a result, the successful numbers of the constant value attack are only 5 and 6 for the two GNSS receivers, and the successful numbers of the exponential value attack are only 6 and 7. Moreover, only 9 and 12 attacks can be successful in the whole interval for the two GNSS receivers with the model of the Fusion-ripper. In contrast, with the scenario classification model, the numbers of successful attacks increase to 36 and 41, respectively.

Scenario 2:

The second scenario is in Whampoa. The vehicle starts in an open-sky environment close to the sea. Then, the vehicle enters a narrow street along a wide road with two lanes adjacent to buildings. Due to the poor sky view, the GNSS cannot achieve trustworthy accuracy in this scenario. Moreover, there is a trajectory section where the vehicle passes through a tunnel. The trajectory and velocity information of the vehicle and the sky visibility information of this scenario is shown in Fig.10(A) and Fig.10(B).

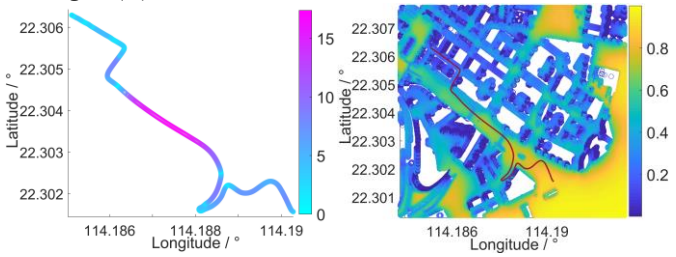
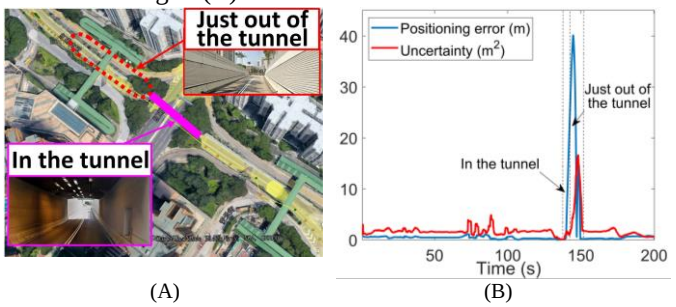


Fig.10. The velocity and sky visibility information of the vehicle.

From the results, the sky visibility information cannot indicate the degree of shading of the vehicle in the tunnel. Therefore, some separate labels are required for the tunnel-related spoofing scenario. In this trajectory, the area where the vehicle passes through the tunnel is shown in Fig.11(A). We present the positioning errors and uncertainties of the LiDAR, as shown in Fig.11(B).



(A) (B)

Fig.11. (A) is the real tunnel scene from Google Earth. (B) is positioning errors and uncertainties of LiDAR in Scenario 2.

From the results, the uncertainty of LiDAR will become larger when the vehicle is just out of the tunnel. So, it is a better scenario to perform a GNSS attack. The final results of scenario classification models are shown in Fig.12.

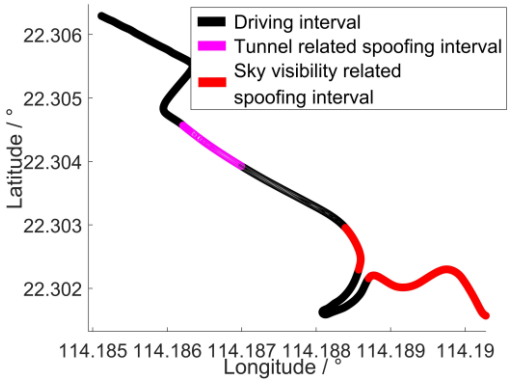


Fig.12. High-risk attack interval for scenario 2. The sky visibility-related interval (the red route) and the tunnel-related interval (the pink route) are the high-risk attack area, and the black trajectory is the area unfavorable to attack.

We specifically select the open-sky area (the red route) and the tunnel-related area (the pink route) to perform an aggressive GNSS spoofing attack. The experimental conditions are the same as in Scenario 1. The results show that the successful numbers of the constant value attack are only 8 and 10 for the two GNSS receivers, and the successful numbers of the exponential value attack are only 12 and 14. Moreover, only 18 and 19 attacks can be successful in the whole interval for the two types of GNSS receivers with the model of the Fusion-ripper. In contrast, with the scenario classification model, the numbers of successful attacks are 37 and 38, respectively.

Finally, the success rate will eventually be calculated by the ratio of the number of successful spoofing n and the total number of spoofing N, which can be expressed as:

$$s = \frac{n}{N} \times 100\% \tag{18}$$

We calculate the spoofing success rate for the two scenarios, as shown in Fig.13. The spoofing success rate of the proposed method (about 75%) can be significantly improved compared with the traditional attack models (less than 40%).

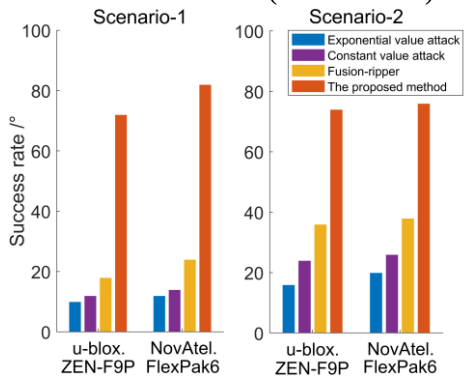


Fig.13. Spoofing success rate of different GNSS spoofing attack models in the two scenarios.

Furthermore, some details should be noted from the experimental results.

1) The spoofing success rate of GNSS receiver NovAtel FlexPak6 is significantly higher than that of u-blox ZED-F9P. This is because the signal of NovAtel FlexPak6 has higher

accuracy and lower uncertainty, so it has higher influence on the position information when the MSF system is spoofed.

2) There are some open-sky areas in the two scenarios selected, that is, the areas with low GNSS and high LiDAR uncertainty or the victim just exiting the tunnel. If the vehicle always runs in a relatively deep urban area, it is possible to fail to find a high-risk scenario.

In conclusion, the attack algorithm based on the scenario classification model is eventually validated by the real data with simulated spoofing attacks from different scenarios. Therefore, the experiment results in this section effectively validate the proposed GNSS spoofing attack model based on scenario classification models in Section III and Section IV.

VI. Conclusion

Different from the state-of-the-art method that performs all kinds of attempted spoofing attacks all the time, we take more steps to propose a spoofing attack scheme based on the scenario classification model in this paper. Attackers can perform efficient GNSS spoofing attacks based on sky visibility and tunnel information. Compared with the traditional models, the proposed scheme can actively select high-risk scenarios and better timing when the victim is in a scenario with high GNSS quality and poor LiDAR signal quality. Finally, the proposed GNSS spoofing attack algorithm for MSF systems is verified via real data with simulated spoofing attacks in different urban scenarios. The success rate can increase to 75% approximately. Therefore, the results show that the proposed scheme significantly improves the success rate of GNSS spoofing attacks.

References

[1] P. Yang, D. Duan, C. Chen, X. Cheng, and L. Yang, "Multi-Sensor Multi-Vehicle (MSMV) Localization and Mobility Tracking for Autonomous Driving," in IEEE Transactions on Vehicular Technology, vol. 69, no. 12, pp. 14355-14364, Dec. 2020.

[2] W. Brenner and A. Herrmann, "An overview of technology, benefits, and impact of automated and autonomous driving on the automotive industry, " in Digital marketplaces unleashed, 2018: 427-442.

[3] Q. Luo, Y. Cao, J. Liu, and A. Benslimane, "Localization and Navigation in Autonomous Driving: Threats and Countermeasures, " in IEEE wireless communications, vol. 26, no. 4, pp. 38–45, 2019.

[4] Q. Li, L. Chen, M. Li, S. -L. Shaw and A. Nüchter, "A Sensor-Fusion Drivable-Region and Lane-Detection System for Autonomous Vehicle Navigation in Challenging Road Scenarios," in IEEE Transactions on Vehicular Technology, vol. 63, no. 2, pp. 540-555, Feb. 2014.

[5] C. Sanders and Y. Wang, "Localizing Spoofing Attacks on Vehicular GPS Using Vehicle-to-Vehicle Communications," in IEEE Transactions on Vehicular Technology, vol. 69, no. 12, pp. 15656-15667, Dec. 2020.

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

[7] Y. Cao et al., "Adversarial Sensor Attack on LiDAR-based Perception in Autonomous Driving, " in Proceedings of the 2019 ACM SIGSAC conference on computer and communications security, 2019: 2267-2281.

[8] J. Sun, "Towards Robust LiDAR-based Perception in Autonomous Driving: General Black-box Adversarial Sensor Attack and Countermeasures, " in 29th USENIX Security Symposium (USENIX Security 20), 2020: 877-894.

[9] K. Eykholt et al., "Robust Physical-World Attacks on Deep Learning Visual Classification, " in CVPR 2018: 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2018, pp. 2087–1634,

[10] Z. Kong, J. Guo, A. Li, et al., "Physgan: Generating physical-world-resilient adversarial examples for autonomous driving, " in Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2020: 14254-14263.

[11] Y. Tu, "Injected and Delivered: Fabricating Implicit Control over Actuation Systems by Spoofing Inertial Sensors," in 27th USENIX Security Symposium (USENIX Security 18), 2018: 1545-1562.

[12] T. Trippel, O. Weisse, W. Xu, et al., "WALNUT: Waging doubt on the integrity of MEMS accelerometers with acoustic injection attacks," in 2017 IEEE European symposium on security and privacy, IEEE, 2017: 3-18.

[13] K. Ren, Q. Wang, C. Wang, et al., "The security of autonomous driving: Threats, defenses, and future directions," in Proceedings of the IEEE," 2019, 108(2): 357-372.

[14] X. Li and W. Zhang, "An Adaptive Fault-Tolerant Multi-sensor Navigation Strategy for Automated Vehicles," in IEEE Transactions on Vehicular Technology, vol. 59, no. 6, pp. 2815-2829, July 2010.

[15] Z. Wang, R. Liu, Q. Liu, L. Han and J. S. Thompson, "Feasibility Study of UAV-Assisted Anti-Jamming Positioning," in IEEE Transactions on Vehicular Technology, vol. 70, no. 8, pp. 7718-7733, Aug. 2021.

[16] J. Xie, Q. Liu, L. Wang, Y. Gong, and Z. Zhang, "Localizing GNSS Spoofing Attacks Using Direct Position Determination," in IEEE Sensors Journal, vol. 22, no. 15, pp. 15323-15333, 1 Aug.1, 2022.

[17] J. Su, J. He, P. Cheng, and J. Chen, "A Stealthy GPS Spoofing Strategy for Manipulating the Trajectory of an Unmanned Aerial Vehicle, " in IFAC-Papers on Line vol. 49, no. 22, pp. 291-296, 2016.

[18] K. (Curtis) Zeng, "All Your GPS Are Belong to Us: Towards Stealthy Manipulation of Road Navigation Systems, " in 27th USENIX security symposium (USENIX security 18). 2018: 1527-1544.

[19] A. John, "Vulnerability Assessment of The Transportation Infrastructure Relying on The Global Positioning System, Final Report," in Volpe National Transportation Systems Center, August 29, 2001, pp. 6 - 88.

[20] S. Warner, G. Johnston R, "A simple demonstration that the global positioning system (GPS) is vulnerable to spoofing," in Journal of security administration, 2002, 25(2): 19-27.

[21] C4ADS, “Above Us Only Stars - Exposing GPS Spoofing in Russia and Syria,” https://www.c4reports.org/aboveusonlystars.

[22] E. Schmidt, Z. Ruble, D. Akopian and D. J. Pack, "Software-Defined Radio GNSS Instrumentation for Spoofing Mitigation: A Review and a Case Study," in IEEE Transactions on Instrumentation and Measurement, vol. 68, no. 8, pp. 2768-2784, Aug. 2019.

[23] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, “Unmanned Aircraft Capture and Control Via GPS Spoofing,” in Journal of field robotics., vol. 31, no. 4, pp. 617–636, 2014.

[24] K. Wang, S. Chen, A. Pan, “Time and position spoofing with open-source projects,” in black hat Europe, 2015, 148: 1-8.

[25] G. Zhang, W. Wen, B. Xu and L. -T. Hsu, "Extending Shadow Matching to Tightly-Coupled GNSS/INS Integration System," in IEEE Transactions on Vehicular Technology, vol. 69, no. 5, pp. 4979-4991, May 2020.

[26] W. Wen, X. Bai, Y. C. Kan and L. -T. Hsu, "Tightly Coupled GNSS/INS Integration via Factor Graph and Aided by Fish-Eye Camera," in IEEE Transactions on Vehicular Technology, vol. 68, no. 11, pp. 10651-10662, Nov. 2019.

[27] 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," in IEEE Sensors Journal, vol. 22, no. 9, pp. 8633-8647, 1 May 2022.

[28] X. Shang, F. Sun, B. Liu, et al., "GNSS Spoofing Mitigation with a Multicorrelator Estimator in the Tightly Coupled INS/GNSS Integration," in IEEE Transactions on Instrumentation and Measurement, 2022.

[29] P. F. Swaszek, "GNSS Spoof Detection Using Shipboard IMU Measurements," in Proceedings of the 27th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2014). 2014.

[30] M. Ceccato, F. Formaggio, N. Laurenti, et al., "Generalized likelihood ratio test for GNSS spoofing detection in devices with IMU," in IEEE Transactions on Information Forensics and Security, 2021, 16: 3496-3509.

[31] C. Tanil, S. Khanafseh, M. Joerger, and B. Pervan, “An INS Monitor to Detect GNSS Spoofers Capable of Tracking Vehicle Position,” in IEEE Transactions on Aerospace and Electronic Systems, vol. 54, no. 1, pp. 131–143, 2018.

[32] Y. Guo, M. Wu, K. Tang, J. Tie and X. Li, "Covert Spoofing Algorithm of UAV Based on GPS/INS-Integrated Navigation," in IEEE Transactions on Vehicular Technology, vol. 68, no. 7, pp. 6557-6564, July 2019.

[33] X. Geng, Y. Guo, K. Tang, et al., "Research on covert directional spoofing method for INS/GNSS Loosely integrated navigation," in IEEE Transactions on Vehicular Technology, 2022.
[34] S. Narain, A. Ranganathan, and G. Noubir, "Security of GPS/INS Based On-road Location Tracking Systems," in 2019 IEEE Symposium on Security and Privacy (SP), 2019, pp. 587–601.
[35] W. Zhao, S. Han, W. Meng, D. Sun and R. Q. Hu, "BSDP: Big Sensor Data Preprocessing in Multi-Source Fusion Positioning System Using Compressive Sensing," in IEEE Transactions on Vehicular Technology, vol. 68, no. 9, pp. 8866-8880, Sept. 2019.
[36] J. Shen, "Drift with Devil: Security of Multi-Sensor Fusion based Localization in High-Level Autonomous Driving under GPS Spoofing," in 29th {USENIX} Security Symposium ({USENIX} Security 20), 2020, pp. 931–948.
[37] Y. Li, C. Wen, F. Juefei-Xu, and C. Feng, "Fooling LiDAR Perception via Adversarial Trajectory Perturbation," in Proceedings of the IEEE/CVF International Conference on Computer Vision, 2021, pp. 514–7887.
[38] Xu Y, Han X, Deng G, et al, "SoK: Rethinking Sensor Spoofing Attacks against Robotic Vehicles from a Systematic View," in arXiv preprint arXiv:2205.04662, 2022.
[39] M. Schreiber, H. Königshof, A.-M. Hellmund, and C. Stiller, "Vehicle Localization with Tightly Coupled GNSS and Visual Odometry," in 2016 IEEE Intelligent Vehicles Symposium (IV), IEEE, 2016.
[40] R. Piché, "Online Tests of Kalman Filter Consistency," in International Journal of Adaptive Control and Signal Processing, vol. 30, no. 1, pp. 115–124, 2016.
[41] J. Chang, L. Zhang, L.-T. Hsu et al., "Analytic Models of a Loosely-coupled GNSS/INS/LiDAR Kalman Filter considering Update Frequency under a Spoofing Attack," in IEEE Sensors Journal, 22.23, 2022, 23341-23355.
[42] Q. Li, J. P. Queralta, T. N. Gia, et al., "Multi-sensor fusion for navigation and mapping in autonomous vehicles: Accurate localization in urban environments," in Unmanned Systems, 2020, 8(03): 229-237.
[43] H. Gao, P. D. Groves, "Environmental context detection for adaptive navigation using GNSS measurements from a smartphone," in Navigation: Journal of the Institute of Navigation, 2018, 65(1): 99-116.
[44] K. Wong, E. Javanmardi, M. Javanmardi, and S. Kamijo, "Estimating Autonomous Vehicle Localization Error Using 2D Geographic Information," in ISPRS Int. J. Geo-Inf., vol. 8, no. 6, p. 288, Jun. 2019.
[45] https://www.td.gov.hk/mini_site/atd/2019/text/tc/section4_1.html
[46] https://zhyue.wikipedia.org/wiki/%E9%A6%99%E6%B8%AF%E9%9A%A7%E9%81%93%E4%B8%80%E8%A6%BD
[47] N. Akai, L. Y. Morales, E. Takeuchi, Y. Yoshihara and Y. Ninomiya, "Robust localization using 3D NDT scan matching with experimentally determined uncertainty and road marker matching," in 2017 IEEE Intelligent Vehicles Symposium (IV), 2017, pp. 1356-1363.
[48] https://earth.google.com/
[49] P. D. Groves, "Shadow matching: A new GNSS positioning technique for urban canyons," in The journal of Navigation, 64(3), 417-430.
[50] M. Magnusson, A. Nuchter, C. Lorken, A. J. Lilienthal and J. Hertzberg, "Evaluation of 3D registration reliability and speed - A comparison of ICP and NDT," in 2009 IEEE International Conference on Robotics and Automation, 2009, pp. 3907-3912.
[51] H. -F. Ng and L. -T. Hsu, "3D Mapping Database-Aided GNSS RTK and Its Assessments in Urban Canyons," in IEEE Transactions on Aerospace and Electronic Systems, vol. 57, no. 5, pp. 3150-3166, Oct. 2021.
[52] J. Zhang, et al., "GNSS-RTK Adaptively Integrated with LiDAR/IMU Odometry for Continuously Global Positioning in Urban Canyons," in Applied Sciences 12.10 (2022): 5193.
[53] M. J. L. Lee, et al., "Skymask matching aided positioning using sky-pointing fisheye camera and 3D City models in urban canyons," in Sensors 20.17 (2020): 4728.
[54] F. Huang, et al., "Point wise or Feature wise? Benchmark Comparison of Public Available LiDAR Odometry Algorithms in Urban Canyons," in arXiv preprint arXiv:2104.05203 (2021).
[55] A. Carballo, A. Monrroy, D. Wong, et al., "Characterization of multiple 3D LiDARs for localization and mapping using normal distributions transform," in arXiv preprint arXiv:2004.01374, 2020.
[56] G. Yan, Y. Deng, "Review on practical Kalman filtering techniques in traditional integrated navigation system," in Navig. Position. Timing, 2020, 7: 50-64.
[57] L.-T. Hsu et al., "UrbanNav: An open-sourced multisensory dataset for benchmarking positioning algorithms designed for urban areas," in Proceedings of the 34th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2021), 2021, pp. 226-256.
[58] T. Takasu,"RTKLIB ver. 2.4. 2 Manual," in RTKLIB: An Open Source Program Package for GNSS Positioning, 2013, 29: 49.
[59] P. Teunissen, "A canonical theory for short GPS baselines. Part I: The baseline precision," in Journal of Geodesy 71, 320–336 (1997).
[60] G. Wan et al., "Robust and Precise Vehicle Localization Based on Multi-Sensor Fusion in Diverse City Scenes," in 2018 IEEE International Conference on Robotics and Automation (ICRA), 2018, pp. 4670-4677.
[61] A. Carballo, A. Monrroy, D. Wong, et al., "Characterization of multiple 3D LiDARs for localization and mapping using normal distributions transform," in arXiv preprint arXiv:2004.01374, 2020.

Jiachong Chang received his B.S. degree from the Department of Automation, Harbin Engineering University in 2016 and the M.S. degree from the School of Instrumentation Science and Engineering, Harbin Institute of Technology in 2018. He is a Ph.D. student in the School of Instrumentation Science and Engineering, Harbin Institute of Technology, and the Department of Aeronautical and Aviation Engineering, Hong Kong Polytechnic University. His current research interests include Multi-sensors fusion, fault diagnosis technology, GNSS spoofing attack.

Feng Huang received his bachelor's degree from Shenzhen University in Automation in 2014 and MSc in Electronic Engineering at Hong Kong University of Science and Technology in 2016. He is a Ph.D. student in the Department of Aeronautical and Aviation Engineering, Hong Kong Polytechnic University. His research interests including localization and sensor fusion for autonomous driving.

Liang Zhang received a Ph.D. degree in Instruments Science and Technology from Southeast University in 2021 and an M.S. degree in Navigation, Guidance, and Control from Nanjing University of Aeronautics and Astronautics in 2017. He was a Postdoctoral Fellow at the Department of Aeronautical and Aviation Engineering of the Hong Kong Polytechnic University in 2022. He is currently a lecturer at the School of Instrument Science and Engineering, Southeast University. His research interest includes inertial navigation, integrated navigation technology, and underwater positioning technology.

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 algorithm, satellite navigation, robust filtering algorithm.

Dr. Li-Ta Hsu received his B.S. and Ph.D. degrees in aeronautics and astronautics from National Cheng Kung University, Taiwan, in 2007 and 2013, respectively. He is currently an associate professor with the Department of Aeronautical and Aviation Engineering. The Hong Kong Polytechnic University, before he served as a post-doctoral researcher in the Institute of Industrial Science at the University of Tokyo, Japan. In 2012, he was a visiting scholar at University College London, the U.K. His research interests include GNSS positioning in challenging environments and localization for pedestrians, autonomous driving vehicle, and unmanned aerial vehicle.