Spoofing Detection for LiDAR in Autonomous Vehicles: A Physical-Layer Approach

Xueyang Hu, Tian Liu, Tao Shu, and Diep Nguyen, *Senior Member, IEEE*

***Abstract*—Recent years have witnessed the ever-growing interest and adoption of autonomous vehicles (AVs), thanks to the latest advancement in sensing and artificial intelligence (AI) technologies. The LiDAR sensor is adopted by most AV manufacturers for its high precision and high reliability. Unfortunately, LiDARs are susceptible to malicious spoofing attacks, which can lead to severe safety consequences for AVs. Most current work focuses on protecting LiDAR against spoofing attacks by using perception model-level defense methods, whose effectiveness unfortunately depends on the correctness of the LiDAR's sensing outcome. A spoofer thus can elude from these methods as long as it fabricates points that maintain the right contextual relationship held by the legitimate points. In this article, we propose to use the signal's Doppler frequency shift to verify the sender of the signal and detect potential spoofing attacks. To this end, we first thoroughly analyze the working principle of LiDAR and conduct real-world experiments to deeply understand and reveal the vulnerability of LiDAR sensors. We then prove that the Doppler frequency shifts of legitimate and spoofing signals present different characteristics, which can be used to fundamentally protect the LiDAR sensing outcome. For better demonstration purposes, we consider three attack models, including static attacker, moving attacker, and moving attacker with control of both velocity and signal frequency. For each of the models, we first show how the spoofing attack is performed and then present our countermeasures. We then propose a statistical spoofing detection framework to jointly consider the impact of short-term uncertainty in vehicle velocity, which can provide more accurate spoofing detection results in realistic environments. Extensive numerical results are provided in a wide range of settings and road conditions.**

***Index Terms*—Connected autonomous vehicles (CAV), Doppler shift, light detection and ranging sensor (LiDAR) sensor, physical-layer security, spoofing attack.**

I. Introduction

IN RECENT years, the development of autonomous vehicles (AVs), i.e., vehicles that can drive by themselves without the real-time intervention of human drivers, is rapidly progressing with the advancement of sensing and artificial intelligence (AI) technologies [1], [2]. Some AVs are already operating on public roads, e.g., Google's Waymo One self-driving taxis [3]. For all these AVs, *driving safety* is always the No.1 requirement. To this end, all existing AVs are equipped with certain types of environment-perception sensors, such as cameras, mmWave radar, ultrasonic sensors, and light detection and ranging sensor (LiDAR). With the rise of the Internet of Things (IoT), AVs can connect to other devices and systems, such as traffic lights and road sensors, to collect real-time data and make more informed decisions. This can enhance the accuracy of the AVs' sensing and decision-making abilities, leading to improved safety and efficiency. Additionally, IoT-enabled AVs can communicate with each other, allowing them to coordinate their movements and further improve safety on the road.

Among the various environment-perception sensors used by AVs, LiDAR sensor is adopted by almost all AV manufacturers due to its high precision and high reliability [4], [5], [6]. The LiDAR sensor employs highly directional laser pulses to probe the surrounding environment. An accurate depth image of the surrounding objects is then collected by the time of flight (ToF) of the received pulse, on which a high-resolution 3-D point cloud map of the environment can be built. In addition, the usage of an infrared laser signal not only makes LiDAR less affected by ambient light in the environment, but also enables LiDAR to remain functional even under poor light conditions.

Ensuring correct and truthful sensing outcome from all environment-perception sensors is essential to ensure reliable safety-critical decision making in autonomous driving. Unfortunately, recent studies have found that LiDARs are susceptible to malicious spoofing attacks that aim to alter LiDAR's sensing outcome by adding fake objects to and removing real objects from the LiDAR's sensed point cloud map, and hence leading to severe safety consequences. For example, the feasibility of injecting fake points into the LiDAR's sensed point cloud was first demonstrated in [7]. They showed that LiDAR sensing results can be easily manipulated by a black-box attack using low-cost commodity hardware (less than 60 U.S. dollars). Subsequent work in [8] launched LiDAR spoofing attacks that successfully fooled a real-world AV perception system, Baidu Apollo 2.5, to detect (faked) objects that do not actually exist in reality. The work in [9] further demonstrated that by spoofing only a small number of points (up to 100), the LiDAR object detection system can be fooled to detect nonexisting objects. Their work shows the severity of the threats posed by spoofing attacks on AV

Manuscript received 6 December 2023; revised 15 January 2024; accepted 25 February 2024. Date of publication 28 February 2024; date of current version 23 May 2024. This work was supported in part by the United States National Science Foundation (NSF) under Grant CNS-2308761 and Grant CNS-2006998. *(Corresponding author: Tao Shu.)*

Xueyang Hu and Tao Shu are with the Computer Science and Software Engineering Department, Auburn University at Auburn, Auburn, AL 36849 USA (e-mail: xueyang.hu@auburn.edu; tshu@auburn.edu).

Tian Liu is with the Research Center of Intelligent Computing Infrastructure Innovation, Zhejiang Laboratory, Hangzhou 311121, China (e-mail: tianliu@zhejianglab.com).

Diep Nguyen is with the School of Electrical and Data Engineering, University of Technology Sydney, Ultimo, NSW 2007, Australia (e-mail: diep.nguyen@uts.edu.au).

Digital Object Identifier 10.1109/JIOT.2024.3371378

LiDARs, which urgently calls for promising countermeasures that can better guarantee the safety of autonomous driving, so as to offer a peace of mind to users when they are using the technology.

In the last couple of years, many works have been focused on mitigating the *effect* of LiDAR spoofing attack using perception model-level defense methods [10], [11], [12], [13]. For example, the work in [9] proposed CARLO, which harnesses occlusion patterns between objects in the LiDAR point cloud for spoofed vehicle detection. The intuition is that, if there are many LiDAR points appearing to pass through a detected object, the object is likely to be a fake object Another anomaly detection system, Shadow-Catcher [14], identifies spoofed ghost objects by checking the contextual consistency between the object and its shadow. Treating the LiDAR's sensed point cloud as a depth image, these methods essentially follow the image-recognition research ideas in AI, which mainly consider the high-level contextual relationship, i.e., the perception, between the points to decide the presence of a spoofer. A critical weakness of these post-sensing methods is that their effectiveness fully depends on the correctness/truthfulness of their input, i.e., the LiDAR's sensing outcome (the point cloud). Therefore, a spoofer will be able to elude from these methods as long as it fabricates/fakes points that maintain the right contextual relationship among them.

Keeping the weakness of the above model-level methods in mind, another category of work is dedicated to fundamentally protect LiDAR from spoofing attacks based on physical-layer authentication (PLA). These methods work on the signal level, and try to authenticate LiDAR's signal based on some physical properties of the light so as to ensure the correctness of LiDAR's sensing outcome. For example, the work in [15] uses amplitude modulation (AM) to directly encrypt LiDAR signals with side channel information leaked from a cryptographic device. Since side channel information cannot be recreated without the knowledge of the secret key, attackers cannot inject spoofing signals while remaining undetected. Meshcheryakov et al. [16] used the signal-to-noise ratio (SNR) of the received signal as an authentication metric and developed a probabilistic approach based on the Neyman–Pearson criterion to select the best SNR threshold for spoofing attack detection. However, a major limitation of their methods is that they use the intensity of the received signal for spoofing detection, which is not a robust metric for LiDARs. In LiDAR sensing, the intensity of the reflected signal faces complicated distortions that are related to the material, size, and roughness of the reflector. Therefore, the sensing signals encrypted by the method in [15] may become unrecognizable after reflections. Furthermore, the SNR of the sensing signal used in [16] has a large variance due to the dynamics of the environment (e.g., reflectors are moving), making it difficult to accurately identify the spoofing signal.

In this article, we find that the intrinsic vulnerability of LiDAR is caused by the fact that current LiDAR sensors blindly accept incoming signals without verifying the sender of the signal. Therefore, we propose to use the signal's Doppler frequency shift to verify the sender of the signal and detect potential spoofing attacks. The fundamental difference between a spoofing signal and a legitimate signal is that the spoofing signal is generated by the attacker and directly sent to the LiDAR receiver, while the legitimate signal is originally sent by the LiDAR transmitter and then echoed/reflected by some objects. Based on this observation and through experiments on real-world testbed, we find that the propagation differences between legitimate and spoofing signals can be characterized by the Doppler shift of the received signal, which can then be used for spoofing attack detection. Specifically, the major contributions of our work are fourfold.

1) To have a deep understanding on the vulnerability of today's LiDAR sensors, we thoroughly analyze the working principle of LiDAR and conduct real-world experiments to demonstrate how easily a spoofing attack can be launched against LiDAR, so as to show such attacks are realistic to current LiDAR technology, and hence the urgency of a promising countermeasure.
2) We prove that the Doppler frequency shifts of legitimate and spoofing signals present different characteristics, and this signal-level difference can be used to fundamentally protect the sensing outcome of LiDAR. We then build a testbed to verify the feasibility of extracting Doppler shift from LiDAR signals with only minor modifications to the LiDAR system. Compared to amplitude and AM-based authentication methods [15], [16], the signal's Doppler frequency shift is a more robust and reliable decision statistic for spoofing detection, because it is decided by the motion between the LiDAR and sensed object and is less affected by the RF environment.
3) To show how the Doppler shift can be used to detect spoofing attacks under different scenarios of attacker capabilities, we thoroughly consider three attack models, including static attacker, moving attacker, and moving attacker with control of both velocity and signal frequency. In each of these models, we first show how spoofing attacks can be performed and then present our countermeasures for spoofing detection.
4) We make the proposed detection mechanisms more accurate and practical by further accounting for the short-term variance/uncertainty in the vehicle's velocity, caused by the vehicle's acceleration and random perturbation on its movement by the road condition. A statistical spoofing detection framework is proposed to jointly consider the impact of velocity and acceleration on the Doppler shift, which can provide more accurate spoofing detection in realistic application environments. Extensive numerical results are provided in a wide range of settings and road conditions.

The remainder of the article is as follows. We begin by briefly reviewing related work in Section II. Then, we analyze the working principle and vulnerability of LiDAR in Section III. We analyze the difference in Doppler frequency shift between legitimate and spoofing signals in Section IV. We consider three attack models and present the spoofing detection method in Section V. The statistic-based spoofing

detection framework is presented in Section VI. And finally, we conclude this article in Section VII.

II. Related Work

A. Attacks Against AV Sensors

Attacks against AV sensors can be classified into three categories according to the physical channel used by the attacker [16], [17], namely, the regular, side, and transmission channel attacks. Regular channel attacks use the same working channel as the sensor (e.g., laser for LiDAR) to directly alter the sensing results. Side channel attacks use a physical channel other than the sensor's working channel to attack the LiDAR [18], [19]. Lastly, transmission channel attacks focus on the transmission channel that connects the sensor and other parts of the system [20], [21], [22].

B. Perception Model Level Defense Methods

Since the point cloud data generated by LiDAR is used by the AI-based perception model for 3-D object detection, many research works focus on mitigating the effect of spoofing attack by the perception model level defense methods. For example, Hau et al. [14] proposed Shadow-Catcher, which validates object identities by examining the shadow of the object in the LiDAR point cloud. The idea is that, for the genuine object representations in the LiDAR point cloud, they are closely followed by regions void of measurements (shadow region). For the injected spoofed object, it is either does not have shadow regions or its shadow regions are inconsistent with the object's size or shape. Zhang et al. [13] and You et al. [23] leveraged the spatio-temporal consistency of the genuine object for spoofing attack detection. The authors utilized a motion prediction framework to analyze the spatio-temporal consistency of objects across consecutive frames in a driving scene. The spoofed object is detected if it violates the law of temporal consistency. However, the major limitation of the above model-level defense methods is that they rely on the geometric formation of points in the LiDAR point cloud and its evolution over time (i.e., the contextual relationship between points) to detect spoofing. These mechanisms first aggregate multiple points in the point cloud to establish an object representation, and then check whether the object representation remains contextually consistent over a certain time period. Therefore, if an attacker can maintain the correct contextual relationship among the fabricated points, it can evade from being detected by these spoofing detection methods. In contrast, our proposed method works in the signal space and evaluates each point in the LiDAR point cloud individually, by testing whether the Doppler shift of the received signal matches with the expected Doppler shift caused by the velocity of the LiDAR. A spoofing LiDAR signal (i.e., a point in the point cloud) causes mismatch between the received Doppler shift and the expected Doppler shift, and hence will be detected by the proposed method, irrespective of its geometric relationship with the other points in the point cloud.

TABLE I
Comparison Between Related Work (Def LV: Defense Method Level, Def Strategies: Defense Strategies, and Phy Inva: Physical Invariants Used)

Def LV	Ref	Attack Model	Phy Inva	Def Strategies
Model	[23]	Add/remove Points in Point-Cloud	N/A	Spatio-temporal Consistency
	[9]			Occlusion Pattern Verification
	[14]			Shadow Pattern Verification
	[13]			Disparity Errors Verification
Transmission	[24]	Data Tamping in Transmission		Dynamic Watermark
	[20]			QIM-based Watermark
Signal	[15]	Change Signal ToF	Amplitude	Signal Amplitude Encryption
	[26]		Time	Challenge-Response Authentication
	[16]		Amplitude	SNR Distribution Analysis
	Ours		**Frequency**	**Doppler Shift Verification**

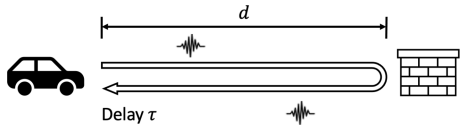


Fig. 1. Normal LiDAR sensing.

C. Signal Level Defense Methods

The signal-level defense method mainly uses PLA for spoofing detection. Unlike perception model-level defense methods, PLA protects LiDAR sensors against spoofing attacks by identifying the malicious signal in the analog domain [24], [25]. The most widely used PLA method is to endow the probes used by active sensors with a special designed feature and use the feature to authenticate the responses. For example, Shoukry et al. [26] proposed PyCRA, which identifies spoofing attacks for magnetic sensors and radio-frequency identification (RFID) tags. PyCRA turns off the probe signal at random instants to verify the existence of any spoofers. If there is no spoofer, it will receive nothing; otherwise, the spoofing attack is identified. However, PyCRA does not meet the high-availability requirement in safety-critical systems, such as an autonomous driving system. When using PyCRA, an AV LiDAR should be turned off at random times for attack detection. As a result, the LiDAR sensor becomes unavailable for environmental sensing during that period, which may cause safety problems for AVs.

For better readability, we summarize the related work in Table I, to highlight the difference between our work and other works.

III. LiDAR Working Principle and Vulnerability

To defend LiDAR against spoofing attack, we first need to understand the working principle and vulnerability of LiDAR. In this section, we first analyze the working principle and vulnerability of LiDAR. Then, we conduct real-world experiments to demonstrate the practicability and easiness of conducting spoofing attacks against LiDAR.

A. LiDAR Working Principle

LiDARs detect and localize objects by actively probing objects with pulses of infrared laser signals between 750 nm to 1.5 μm. Fig. 1 shows a typical LiDAR sensing scenario. A LiDAR sensor consists of two parts: 1) a laser diode as transmitter and 2) a photodetector as receiver. During LiDAR sensing, the transmitter periodically emits laser pulses

to the environment. After the pulses reach the objects in the environment, they are reflected back and received by the LiDAR photodetector. The reflected signals are called echo signals. The time difference between the emitting and arriving time of the signal, i.e., ToF, is used to calculate the distance d between the LiDAR and the object. Let t_s denote the time of the laser pulse being sent by the transmitter, and t_a denote the time of the echo signal being received by the photodetector. The ToF of the received signal τ is $t_a - t_s$, and the distance d between the LiDAR and the detected object is

$$d = \frac{c}{2n}\tau \tag{1}$$

where n is the refractive index of the propagation medium ($n = 1$ for air) and c is the speed of light. By mechanically or electronically steering the laser pulses toward different directions and calculating the ToF distances of the echo signals, LiDAR is able to generate a point cloud, which is a high-resolution depth image of the environment.

B. Motivating LiDAR Security via Real-World Observations

Existing LiDAR only accepts the first arrival signal and uses the signal's arrival time for ToF distance calculation without verifying whether that signal was sent out by the LiDAR's laser diode (i.e., the legitimate transmitter). This leaves a sufficient loophole for many possible forms of spoofing attacks. In the following, we first present a simple toy example implemented in [8] to illustrate a basic type of spoofing attack that fakes a point in the LiDAR point cloud through ToF manipulation. Such a basic attack can be used as building blocks by the attacker to create more sophisticated spoofing attacks, e.g., those that fake an object. We then present our real-world experiments that are built upon two commercial YD X2L LiDARs to demonstrate how spoofing attacks can actually take place in real-world applications. The main purpose of this section is twofold.

1) To better motivate the LiDAR spoofing attack problem studied in this article. In particular, by demonstrating a real LiDAR spoofing attack over a commercially available LiDAR system, we wish to show that such an attack is very realistic for LiDAR systems available in today's market. Note that even though such attacks have been demonstrated in the past, most of them were based on experimental testbeds in a lab rather than directly over a commercially available LiDAR product. We believe that showing the spoofing attack on a commercial LiDAR product will make the attack more convincing, especially for readers not familiar with LiDAR and its vulnerabilities.
2) To better show the compelling nature of the problem: By showing how easy it is to launch a spoofing attack against current LiDARs, we highlight the urgent need for solutions to this compelling security problem.

1) Toy Example for Spoofing Attack: A basic point-faking attack was proposed and implemented in [8], as illustrated in Fig. 2. This system features a photodiode, a time delay component, and a laser diode. The total cost of the system is less than 50 U.S. dollars. The goal of this spoofing system is

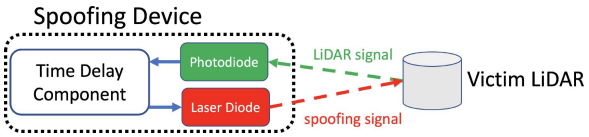


Fig. 2. Spoofing device.

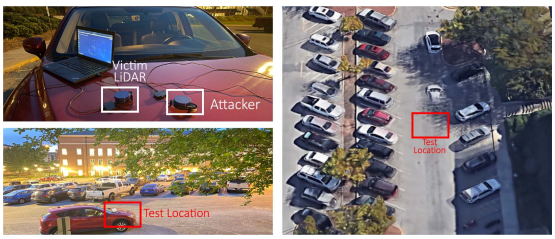


Fig. 3. Outdoor spoofing test environment and setup.

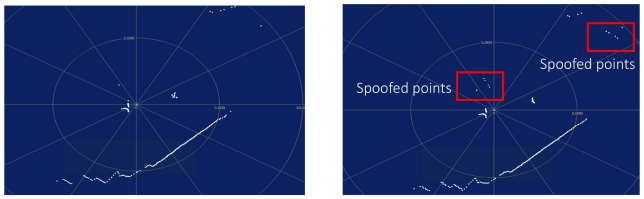
to deceive the LiDAR by sending signals with false ToF that simulate a fake object. The spoofing signal can be injected to LiDAR via an attacker-controlled laser diode, whose working wavelength is the same as the victim's LiDAR. By properly controlling the timing of the spoofing signal, the attacker can alter the ToF measurements of the victim LiDAR, which in turn results in a counterfeit point at the distance that the attacker desires. More specifically, suppose that the attacker aims to mislead the LiDAR in detecting a counterfeit point at distance d_{spoof}, while the actual physical distance between the LiDAR and the attacker is d. To achieve the attack goal, the attacker first needs to synchronize with the victim LiDAR to obtain the sending time of the laser pulses. The attacker then sends a spoofing signal to LiDAR and ensures that the arrival time of the spoofing signal t_a^{spoof} is

$$t_a^{\text{spoof}} = t_s + \tau_{\text{spoof}} \tag{2}$$

where $\tau_{\text{spoof}} = 2d_{\text{spoof}}/c$. In this case, when the spoofing signal is received by LiDAR, the calculated ToF distance between the LiDAR and the attacker is now manipulated to be d_{spoof} (instead of being d), resulting in a faked point in the LiDAR's point cloud.

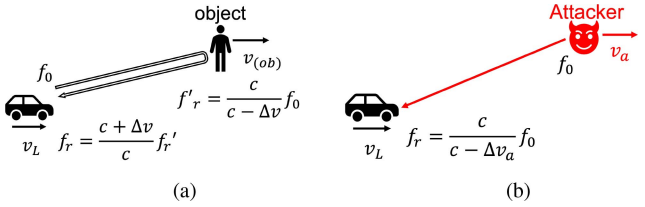
To launch a real-world spoofing attack, the photodiode in Fig. 2 serves as a synchronization device to trigger the delay component whenever it captures laser signals from the victim LiDAR. And the delay component activates the laser diode to send a spoofing signal toward the victim LiDAR after a specified time delay τ_{spoof}.

2) Our Real-World Experiments: To show how easily a spoofing attack can be launched against current LiDAR systems, we conduct the following real-world experiment. We use two YD X2L LiDARs [27]. One of the LiDARs acts as the victim LiDAR to generate point cloud data for the test environment. The other LiDAR is configured as a spoofing attacker that periodically generates spoofing signals with random ToF to attack the victim LiDAR. We conduct our spoofing attack experiments in an outdoor parking lot, and the test environment and test location are shown in Fig. 3. In the test, the victim LiDAR is running normal operation to sense the environment and generate point cloud data, and



(a) (b)

Fig. 4. LiDAR point-cloud data. (a) Normal point cloud. (b) Point cloud under attack.



(a) (b)

Fig. 5. Doppler frequency shift illustration. (a) Normal sensing (round trip). (b) Spoofing attack (single-way).

the spoofing attacker is located 1.5 m away from the victim LiDAR and shooting signals with random time delays.

Fig. 4 shows a comparison of LiDAR point cloud with and without spoofing attack. In Fig. 4(a), the point cloud with no spoofing attack clearly captures the shape and distance of the surrounding objects. In contrast, in Fig. 4(b), there are multiple spoofed points shown on the point cloud map (marked by red squares). It can be seen that under the random attack, two small clusters of spoofed points are generated in the LiDAR point cloud. These clusters of spoofed points may deceive the LiDAR system to misinterpret them as two small objects in front of the LiDAR: one in the 12 o'clock direction and the other in the 2 o'clock direction, which actually do not exist at all in reality. This indeed poses a serious safety threat for the AVs. Note that the experiment in Fig. 4 is just a simple example. In reality, instead of a random attack, the attacker can enhance their attack effects (i.e., generate a bigger cluster of spoofed points in the point cloud) by launching more sophisticated attacks.

IV. Doppler Frequency Shift in LiDAR Sensing

To fundamentally protect LiDAR against spoofing attacks in the analog domain, it is crucial to distinguish legitimate sensing signals and spoofing signals based on signal-level features. However, choosing an appropriate physical feature that can correctly represent the difference between legitimate and spoofing signals is a challenge.

In this section, we first prove that the Doppler frequency shift of the received signal can properly characterize the propagation difference between the legitimate and spoofing signal and distinguish the spoofing signal. Then, we build a real-world testbed to show the practicability of extracting Doppler shift from LiDAR's laser signal.

A. Doppler Frequency Shift Difference Between Legitimate Signal and Spoofing Signal

The Doppler effect, or Doppler frequency shift, is the change in frequency of a signal in relation to the relative movement between the signal's transmitter and receiver. In LiDAR sensing, due to the relative motion between the LiDAR and the detected object, the echoed signal presents a frequency shift caused by the Doppler effect.

In LiDAR sensing, the legitimate sensing signal is sent by LiDAR's transmitter, reflected by an object in the environment and then received by the LiDAR's receiver, which travels through a round trip. Let us consider a 2-D case to derive the Doppler frequency shift of the legitimate sensing signal. Let the velocity vector of LiDAR be $\vec{v}_L$ and the velocity vector of the object detected be $\vec{v}_{(ob)}$. The Doppler shift of the legitimate sensing signal is determined by the relative radial speed between the LiDAR and the object, which is defined as the rate of change of the distance between them. The relative radial speed Δv between the LiDAR and the object is calculated as $\Delta v = (\vec{v}_L - \vec{v}_{(ob)}) \cdot \vec{l}$, where $\cdot$ is the dot product and $\vec{l}$ is the Direction of Arrival (DoA) vector of the signal (i.e., the direction along the line connecting the LiDAR and the detected object). Due to the large magnitude of the speed of light, the DoA of the received signal is considered to be the same as the sending direction of the signal, which is considered as known.

Recall that the legitimate sensing signal travels through a round trip. We introduce an intermediate signal frequency f'_r, which is the frequency of the signal that reaches the object. Let f_0 be the frequency of the signal transmitted by LiDAR and f_r be the frequency of the received signal, as shown in Fig. 5(a). In the forward trip of the round trip, the signal with frequency f_0 is sent to the object, and f'_r is

$$f'_r = \left(\frac{c}{c-\Delta v}\right) f_0. \tag{3}$$

Then, the signal with frequency f'_r is reflected back to LiDAR on the same route, and the received signal frequency f_r is

$$f_r = \left(\frac{c+\Delta v}{c}\right) f'_r. \tag{4}$$

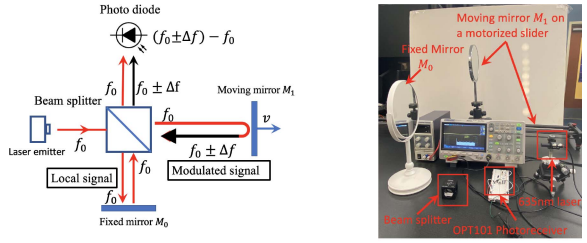
The Doppler frequency shift Δf of the received signal is calculated as the frequency difference between the transmitted and received signals, which is

$$\Delta f = f_r - f_0 = \left(\frac{c+\Delta v}{c-\Delta v} - 1\right) f_0 \approx \frac{2f_0}{c} \Delta v. \tag{5}$$

The approximation is valid since Δv is much smaller than the speed of light c (3×10^8 m/s).

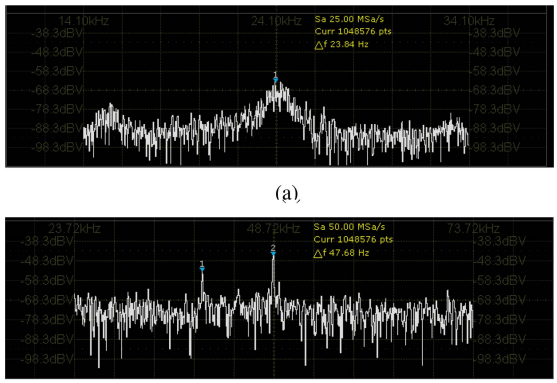
In contrast, the spoofing signal is sent directly to LiDAR by the attacker, which only travels one-way. Let $\vec{v}_a$ be the velocity vector of the attacker. The relative radial speed between the LiDAR and the attacker is $\Delta v_a = (\vec{v}_L - \vec{v}_a) \cdot \vec{l}$, as shown in Fig. 5(b). Since the frequency of the transmitted spoofing signal is also f_0, the Doppler frequency shift of the spoofing signal Δf_a is

$$\Delta f_a = \left(\frac{c}{c-\Delta v_a}\right) f_0 - f_0 = \frac{\Delta v_a}{c-\Delta v_a} f_0 \approx \frac{f_0}{c} \Delta v_a. \tag{6}$$



(a) (b)

Fig. 6. Testbed design. (a) Schematic. (b) Testbed layout.



(a)

(b)

Fig. 7. Doppler shift spectrum results. (a) Δf = 24.10 KHz, $\bar{v}$ = 0.75 cm/s. (b) Δf = 48.72 KHz, $\bar{v}$ = 1.55 cm/s

Based on the above analysis, it is clear that the Doppler shifts of the legitimate and spoofing signals are different due to their different propagation paths: the Doppler frequency shift of the legitimate sensing signal is twice as much as that of the spoofing signal under the same radial speed due to its round trip propagation. As will be elaborated shortly in Section V, the above margin (a factor of 2) between the Doppler frequency shifts of legitimate and spoofing signals can be utilized to construct reliable and accurate spoofing detection mechanisms under various attack conditions.

Next, we present a proof-of-concept testbed to demonstrate the feasibility of extracting Doppler frequency shift from the laser signal of a moving LiDAR.

B. Feasibility Study of Extracting Doppler Frequency Shift

1) Proof-of-Concept Testbed Design: We design and build a proof-of-concept testbed to test the feasibility of extracting the velocity-based Doppler shift from the laser similar in nature to those used in LiDAR systems. The schematic diagram of the testbed is shown in Fig. 6(a). The Doppler shift is extracted by using the self-mixing effect of the signal. Specifically, the laser signal with frequency f_0 is first split into two orthogonal beams by a 3-dB beam splitter in the middle. Then, one beam of signal, which is called the local signal, is reflected back by the fixed mirror M_0. And the other beam of signal, termed the modulated signal, is reflected back by a moving mirror M_2 whose velocity is v. The local signal and the modulated signal are mixed together and received by the photodiode to extract the Doppler frequency shift of the modulated signal.

The Doppler shift of the modulated signal is extracted by the homodyne detection method. The local signal Y_{LO} and the modulated signal Y_M can be expressed as

$$Y_{LO} = A_{LO} \cdot e^{-j(2\pi f_0 t + \phi_{LO})}$$
$$Y_M = A_M \cdot e^{-j(2\pi (f_0 \pm \Delta f) t + \phi_M)}$$

where $A_{LO}, \phi_{LO}, A_M, \phi_M$ denote the amplitude and phase shift of the local and modulated signal, respectively. j is the imaginary unit and $\Delta f = (2v/c)f_0$ is the Doppler frequency shift caused by the movement of the mirror M_1.

The output of the photodetector is the combined signal power of Y_{LO} and Y_M. Due to the low-pass filtering effect of the photodetector, the high-frequency components of $Y_{LO}+Y_M$ are filtered out, and the output power is

$$P_{out} = \frac{A_M^2}{2} + \frac{A_{LO}^2}{2} + A_M A_{LO} \cos(2\pi \Delta f t + \phi_M - \phi_{LO})$$

which is a beat signal with frequency Δf. By filtering out the direct current (DC) signal, Δf can be extracted by fast Fourier transform (FFT).

2) Testbed Implementation: Regarding the implementation of the testbed, we use a 635 nm ThorLabs PL202 laser diode to send laser signals. A cubic beam splitter, ThorLabs CCM1-BS013, is used to split the beam. The photoreceiver is OPT101 from Texas Instruments. The moving mirror is attached to a motorized camera slider for stable and continuous movement. An oscilloscope is connected to the photoreceiver for data collection and visualization. The layout of the testbed is shown in Fig. 6(b).

Note that for the demonstration purpose, we use mirrors instead of real obstacles. In real-world scenarios, the surface roughness and color of the obstacle can affect the received signal's SNR. Rough surfaces can scatter laser light, and darker colors absorb more light, resulting in weaker reflections (i.e., smaller reflection coefficient of the obstacle) and hence lower SNR. However, in practice, the reduced reflection coefficient can be well compensated by using a higher power laser emitter and filter lenses, which are commonly adopted by vehicle LiDARs. Therefore, in real-world use cases, the LiDAR's SNR should be sufficient for reliable and accurate Doppler shift extraction.

3) Test Results: We then use the above testbed to extract the Doppler frequency shift of the received signal and estimate M_1's velocity v. Fig. 7 shows the Fourier spectrum of the signals for different velocities of M_1. In the experiment, the moving speed of M_1 is set to 0.75 cm/s and 1.50 cm/s, respectively. The estimated velocity $\tilde{v}$ of M_1, which is calculated from the Doppler shift Δf, is $\tilde{v} = (\Delta f/2f_0)c$. In Fig. 7(a), the Doppler shift of the signal is 24.10 kHz, which corresponds to $\tilde{v}$= 0.75 cm/s and is match with the M_1's ground truth speed v = 0.75 cm/s. In Fig. 7(b), there are two peaks found, and the peak with the highest value is chosen as the Doppler shift that corresponds to the real signal. In this case, the Doppler frequency of the signal is 48.72 kHz, which corresponds

to $\tilde{v}$= 1.55 cm/s. Under real-world conditions, the Doppler spectrum of the received signal may contain multiple peaks due to random noise and subtle movement of the object. A general principle of identifying the real signal is to choose the frequency component with the highest energy, as this is caused by the dominant movement of the object. Compared to the ground truth speed of $v = 1.50$ cm/s, the small variance between v and $\tilde{v}$ is caused by noise in the photodiode. This small variance does not affect the accuracy of our proposed spoofing attack detection method. As will be shown in later sections, the velocity detection error [about 3% as shown in Fig. 7(b)] caused by random noise is much smaller than the separation between the detected velocity of a real object and the detected velocity of a spoofed object (the former is twice as much as the latter). Furthermore, the impact of random noise can be reduced by our statistical spoofing detection framework presented in Section VI.

In summary, this experiment establishes the feasibility of extracting the Doppler shift of high-frequency LiDAR signals over a testbed that is open for redevelopment. The same structure of the testbed can be integrated into real-world LiDAR systems to extract the Doppler shift and detect spoofing attacks. Specifically, the testbed is based on an interferometer structure and can be integrated into LiDARs. The potential challenges of incorporating our method into the LiDAR system include:

1) *Cost Issue:* Implementing the structure shown in Section IV-B requires an additional frequency mixer and A/D converters, which increases the manufacturing cost of LiDAR sensors.
2) *Standardization Issues:* The lack of industry-wide standards for LiDAR systems can cause compatibility and interoperability issues between different AV models and brands. At this point, all commercial LiDAR products available on the market are proprietary and are not open for redevelopment.

We understand that there have been numerous existing commercial products on the market that are capable of extracting Doppler shift from laser signals. However, these products are often proprietary, and hence are not friendly to redevelopment. The spoofing detection measures developed in the subsequent sections can be implemented on the testbed presented in this section.

V. Doppler Shift-Based Spoofing Detection

In the previous section, we demonstrated that the Doppler shift of the laser signal can be used to distinguish between a spoofing signal and a legitimate sensing signal. In this section, we present the detailed designs that utilize the Doppler frequency shift for LiDAR spoofing attack detection under various attack models. Specifically, we first study the uniform-motion scenario, where the velocities of the attacker, the LiDAR, and genuine objects in the environment are assumed to be constants during the window of detection (we will relax this assumption and consider accelerations in the next section). We consider three different spoofing attack models, respectively: 1) a static attacker; 2) a mobile attacker; and 3) a mobile attacker that controls both its velocity and signal frequency. Each of these models can be considered as a generalization of the model before it. We start off our detection design with the simplest attack model—the static attacker, and gradually make the design more general by considering more realistic conditions in the attack. For each attack model, we first show how the spoofing attacks are performed. Then, we illustrate the countermeasure that uses the signal Doppler shift to identify the spoofing attack.

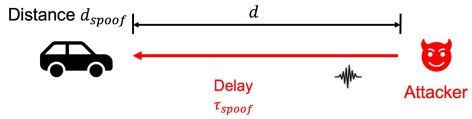


Fig. 8. Spoofing attack in Scenario 1.

We need to point out that the spoofing attack models adopted by the related works are essentially based on the same assumption of the attacker's most basic attack capability considered in this work. In particular, no matter it is the fake object injection attack or the target object removal attack, they are all built upon the attacker's foundational capability of being able to manipulate the time-of-flight of the LiDAR signal, so that the attacker can either inject a fake point into or remove a real point from the LiDAR's point cloud. Our work considers exactly the same foundational capability of the attacker, as shown in Fig. 2 and Section III-B1. In this regard, the comparison between our work and those related works is fair. In addition, our work not only considers the same foundational capability of the attacker, but also studies how such a foundational capability can be achieved by an attacker and how such capability can be countered under various realistic scenarios, e.g., when the attacker is static, or when the attacker is mobile, or when the attacker can control its movement and the frequency of the LiDAR signal, etc. Because the detection methods proposed in our work essentially target detecting the manipulation of the time-of-flight of the LiDAR signals, they are also able to detect those fake object injection attacks and the target object removal attacks which are based on the above manipulations.

A. Attack Model 1 (Static Attacker and Moving LiDAR)

1) Spoofing Attack in Model 1: We first consider the case where only LiDAR is moving with constant velocity $\vec{v}_L$, and any other objects and the attacker remain static. This is a common scenario for LiDAR spoofing attacks. For example, the attacker can place the spoofing device on the roadside to shoot malicious laser pulses to AVs passing by. We also assume that the LiDAR system already knows that all genuine objects are static. In this scenario, similar to the example illustrated in Section III-B1, the attacker aims to mislead the LiDAR in detecting a counterfeit point at distance d_{spoof} while the real distance between the LiDAR and the attacker is d. This is achieved by sending spoofing signal with time delay τ_{spoof} to the victim LiDAR, as shown in Fig. 8.

In this attack scheme (and also the subsequent two attack models), it is assumed that the attacker is aware of the working frequency of the victim LiDAR, and the transmitted spoofing signal has the same frequency as the victim LiDAR's working

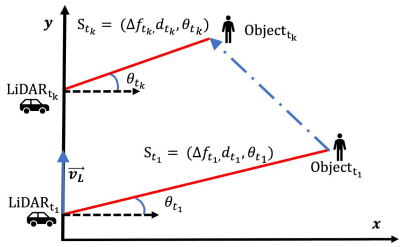


Fig. 9. Cartesian coordinate system and signal tuple.

frequency. This assumption is practical because the working frequency of a vehicle's LiDAR can be easily obtained through the product specification. We also assume that the attacker is aware of its distance to the victim LiDAR, so that it can decide the timing of emitting the spoofing signal that misleads the victim LiDAR to calculate d_{spoof}. This assumption is reasonable because the attacker can simply use its own LiDAR to monitor its distance to the victim in real time.

2) Spoofing Detection in Attack Model 1: In Attack Model 1, a spoofing signal can be identified by testing whether the Doppler shift of the received signal matches the expected Doppler shift caused by the velocity of the LiDAR. Specifically, for the legitimate sensing signal sent to direction $\vec{l}$, since only LiDAR is moving with velocity $\vec{v}_L$, the expected Doppler frequency shift of the reflected signal is $(2f_0/c)\vec{v}_L \cdot \vec{l}$. Here, due to the small field of view of LiDAR receiver (less than 1°), the transmission direction of the signal is the same as the receive direction. Let the Doppler shift of the received signal be Δf_r (Δf_r can be measured as illustrated in Section IV-B). To detect a spoofing signal, the following should be tested:

$$\Delta f_r \stackrel{?}{=} \frac{2f_0}{c}\left(\vec{v}_L \cdot \vec{l}\right). \tag{7}$$

For the spoofing signal sent by the attacker from direction $\vec{l}$, since the attacker is static and the spoofing signal travels one way, its Doppler shift is only $(f_0/c)\vec{v}_L \cdot \vec{l}$—a margin of a factor of 2. Therefore, the spoofing signal can be detected.

B. Attack Model 2 (Moving Attacker and Moving LiDAR)

Next, we consider a more general attack model, where the LiDAR, the attacker, and the object in the environment are moving. This scenario is more common than attack model 1. For example, the attacker can drive a vehicle in close proximity to the victim AV, e.g., in the same lane or adjacent lanes, to shoot the laser pulses to the victim AV's LiDAR. To better present the spoofing attack and the proposed spoofing detection in this model, we first introduce some basic notation and definitions.

Let us consider a 2-D Cartesian coordinate system shown in Fig. 9. Let the LiDAR's velocity be $\vec{v}_L$. Without loss of generality, we assume that the direction of $\vec{v}_L$ is the same as the y-axis, and the x-axis is perpendicular to $\vec{v}_L$. With the movement of the LiDAR and the object, the LiDAR receives a series of signals emitted by the LiDAR and then reflected by the object at different locations. In particular, at times $t_1, t_2, \ldots, t_K$, let the locations of the LiDAR and the object be LiDAR_{t_1}, Object_{t_1}, LiDAR_{t_2}, Object_{t_2}, …, and LiDAR_{t_K}, Object_{t_K}, respectively. Denote the signal that is emitted from the LiDAR, reflected by the object, and then received by the LiDAR at time t_k by S_{t_k}, where $k = 1, 2, \ldots, K$. The signal S_{t_k} can be presented as a tuple $S_{t_k} = [\Delta f_{t_k}, d_{t_k}, \theta_{t_k}]$, where Δf_{t_k}, d_{t_k}, and θ_{t_k} represent the signal's Doppler frequency shift, ToF distance, and Angle of Arrival (AoA), respectively, at time t_k, as shown in Fig. 9. Let $\mathbb{S}$ denote the set of signals reflected by the object and received by the LiDAR from time t_1 to time t_K.

Using $\mathbb{S}$, we can determine the velocity of the object in one of two ways: 1) by the signal's Doppler shift or 2) by the ToF distance. We refer to the velocity determined from the ToF distance as the object's ToF velocity, and the velocity determined by the Doppler frequency shifts as the Doppler velocity. More specially, these velocities can be calculated as follows.

ToF Velocity: The ToF velocity of the object, denoted as $\vec{v}_{\text{ToF}}$, can be determined based on the ToF distances of the signals. In particular, the velocity vector can be represented as $\vec{v}_{\text{ToF}} = |\vec{v}_{\text{ToF}}|(\cos\phi_{\text{ToF}}, \sin\phi_{\text{ToF}})$, where $|\vec{v}_{\text{ToF}}|$ and ϕ_{ToF} denote the magnitude and direction angle of $\vec{v}_{\text{ToF}}$. Given any two signals received at time t_m and t_n ($t_m < t_n$), i.e., $S_{t_m} = [\Delta f_{t_m}, d_{t_m}, \theta_{t_m}]$ and $S_{t_n} = [\Delta f_{t_n}, d_{t_n}, \theta_{t_n}]$, $\vec{v}_{\text{ToF}}$ can be calculated as

$$|\vec{v}_{\text{ToF}}| = \Big[(d_{t_n}\sin\theta_{t_n} - d_{t_m}\sin\theta_{t_m})^2 + (d_{t_n}\cos\theta_{t_n} + |\vec{v}_L|\Delta t - d_{t_m}\cos\theta_{t_m})^2\Big]^{\frac{1}{2}} \tag{8}$$

and

$$\phi_{\text{ToF}} = \arctan\frac{d_{t_n}\cos\theta_{t_n} + |\vec{v}_L|\Delta t - d_{t_m}\cos\theta_{t_m}}{d_{t_n}\sin\theta_{t_n} - d_{t_m}\sin\theta_{t_m}} \tag{9}$$

where $\Delta t = |t_n - t_m|$.

Doppler Velocity: The object's Doppler velocity $\vec{v}_{\text{Dop}}$, can be represented as $\vec{v}_{\text{Dop}} = |\vec{v}_{\text{Dop}}|(\cos\phi_{\text{Dop}}, \sin\phi_{\text{Dop}})$, where $|\vec{v}_{\text{Dop}}|$ and ϕ_{Dop} are the magnitude and direction angle of the velocity. Given two signals $S_{t_m} = [\Delta f_{t_m}, d_{t_m}, \theta_{t_m}], S_{t_n} = [\Delta f_{t_n}, d_{t_n}, \theta_{t_n}] \in \mathbb{S}$, $|\vec{v}_{\text{Dop}}|$ and ϕ_{Dop} can be calculated by solving the following set of nonlinear equations:

$$\begin{cases} |\vec{v}_L|\sin(\theta_{t_m}) - |\vec{v}_{\text{Dop}}|\cos(\theta_{t_m} - \phi_{\text{Dop}}) = \frac{c}{2f_0}\Delta f_{t_m} \\ |\vec{v}_L|\sin(\theta_{t_n}) - |\vec{v}_{\text{Dop}}|\cos(\theta_{t_n} - \phi_{\text{Dop}}) = \frac{c}{2f_0}\Delta f_{t_n}. \end{cases} \tag{10}$$

Depending on whether the attacker controls its velocity to facilitate the spoofing, the attacker's spoofing attack schemes can be divided into the following two cases.

1) Spoofing Attack When Attacker Does Not Control Its Velocity: We first consider a simple spoofing attack in which the attacker only manipulates the ToF distance of the probing signal, but does not control its velocity to facilitate the attack. Specifically, to launch a spoofing attack, the attacker injects spoofing signals into the victim LiDAR so that the legitimate signal set $\mathbb{S}$ that corresponds to a genuine object is replaced by the spoofing signal set $\mathbb{S}^{(\text{spf})}$, where $S_{t_k}^{(\text{spf})} = [\Delta f_{t_k}^{(\text{spf})}, d_{t_k}^{(\text{spf})}, \theta_{t_k}] \in \mathbb{S}^{(\text{spf})}$. Note that due to the small field of view of the LiDAR receiver, the spoofing signal can only be injected when the LiDAR is transmitting to and receiving from the attacker's direction, and the AoAs of the spoofing

signal can not be changed by the attacker. The goal of the attacker is to mislead the LiDAR's calculation of its distance to the faked object by manipulating $d_{t_k}^{(\text{spf})}$, similar to that in Section V-A1. The ToF of the spoofing signal is determined by the attacker according to its attack goal, i.e., how far does it want the faked object to be from the LiDAR, based on (2).

2) Spoofing Detection When Attacker Does Not Control Its Velocity: The key insight in the above attack model is that $\Delta f_{t_k}^{(\text{spf})}$ and $d_{t_k}^{(\text{spf})}$ are not independent between each other. This is because both quantities are related to the velocity of the attacker/faked object, and both can be used to calculated that velocity according to (8)–(10). Since the attacker does not adjust its velocity according to the ToF distance it claims to be, there exists a mismatch between the Doppler velocity $\vec{v}_{\text{Dop}}$ and the ToF velocity $\vec{v}_{\text{ToF}}$. This allows us to detect spoofing by testing the following:

$$\vec{v}_{\text{ToF}} \stackrel{?}{=} \vec{v}_{\text{Dop}}. \tag{11}$$

For legitimate signals reflected by genuine objects, its ToF distance is authentic (i.e., not manipulated), and therefore $\vec{v}_{\text{Dop}} = \vec{v}_{\text{ToF}}$. Otherwise, a mismatch indicates the presence of a spoofing attack.

3) Spoofing Attack When Attacker Controls Its Velocity: An attacker can tailor its velocity to its claimed ToF distance to ensure that the calculated Doppler velocity $\vec{v}_{\text{Dop}}$ matches the ToF velocity $\vec{v}_{\text{ToF}}$. In particular, this can be achieved according to the following.

Proposition 1: Given the attacker's velocity $\vec{v}_a = |\vec{v}_a|(\cos\phi_a, \sin\phi_a)$, where ϕ_a is the direction angle of $\vec{v}_a$, to maintain consistency between the Doppler velocity and ToF velocity of the spoofing signals, for any two spoofing signals $S_{t_m}^{(\text{spf})}, S_{t_n}^{(\text{spf})} \in \mathbb{S}^{(\text{spf})}$, where $S_{t_m}^{(\text{spf})} = [\Delta f_{t_m}^{(\text{spf})}, d_{t_m}^{(\text{spf})}, \theta_{t_m}]$ and $S_{t_n}^{(\text{spf})} = [\Delta f_{t_n}^{(\text{spf})}, d_{t_n}^{(\text{spf})}, \theta_{t_n}]$, $\theta_{t_m} \neq \theta_{t_n}$, $d_{t_m}^{(\text{spf})}$ and $d_{t_n}^{(\text{spf})}$ must satisfy the following equation set:

$$d_{t_m}^{(\text{spf})} = \frac{\cos(\theta_{t_n})|\vec{v}_L|\Delta t + \frac{f(\theta_{t_m})\sin(\theta_{t_n}-\Phi)}{2\cos(\theta_{t_m}-\phi_a)}\Delta t}{\sin(\theta_{t_n}-\theta_{t_m})} \tag{12}$$

$$d_{t_n}^{(\text{spf})} = \frac{\cos(\theta_{t_m})|\vec{v}_L|\Delta t + \frac{f(\theta_{t_n})\sin(\theta_{t_m}-\Phi)}{2\cos(\theta_{t_n}-\phi_a)}\Delta t}{\sin(\theta_{t_n}-\theta_{t_m})} \tag{13}$$

where

$$f(\theta) = |\vec{v}_L|\sin(\theta) + |\vec{v}_a|\cos(\theta-\phi_a)$$
$$\Phi = \arctan\frac{f(\theta_{t_n}) * \cos\theta_{t_m} - f(\theta_{t_m}) * \cos\theta_{t_n}}{f(\theta_{t_m}) * \sin\theta_{t_n} - f(\theta_{t_n}) * \sin\theta_{t_m}}$$

and $\Delta t = |t_n - t_m|$.

Proof: The ToF velocity derived from the spoofing signals $\vec{v}_{\text{ToF}}$ must be equal to the Doppler velocity of the spoofing signals $\vec{v}_{\text{Dop}}$. Denote $\vec{v}_{\text{Dop}} = |\vec{v}_{\text{Dop}}|(\cos\Phi, \sin\Phi)$. Since the attacker is directly sending the spoofing signals to the victim LiDAR, the Doppler shifts of the spoofing signals are determined by the relative radial velocity between the LiDAR and the attacker. We also have the Doppler shifts of the spoofing signals as

$$\Delta f_{t_m}^{(\text{spf})} = \frac{f_0}{c}(|\vec{v}_L|\sin(\theta_{t_m}) - |\vec{v}_a|\cos(\theta_{t_m}-\phi_\alpha))$$
$$\Delta f_{t_n}^{(\text{spf})} = \frac{f_0}{c}(|\vec{v}_L|\sin(\theta_{t_n}) - |\vec{v}_a|\cos(\theta_{t_n}-\phi_\alpha)).$$

And $\vec{v}_{\text{Dop}}$ can be obtained by substituting $\Delta f_{t_m}^{(\text{spf})}$ and $\Delta f_{t_n}^{(\text{spf})}$ into (10), which gives

$$|\vec{v}_{\text{Dop}}| = \frac{f(\theta_{t_m})}{2\cos(\theta_{t_m}-\Phi)}$$
$$\Phi = \arctan\frac{f(\theta_{t_n}) * \cos\theta_{t_m} - f(\theta_{t_m}) * \cos\theta_{t_n}}{f(\theta_{t_m}) * \sin\theta_{t_n} - f(\theta_{t_n}) * \sin\theta_{t_m}} \tag{14}$$

where $f(\theta)$ is the function value of θ, and we have

$$f(\theta) = |\vec{v}_L|\sin(\theta) + |\vec{v}_a|\cos(\theta-\phi_a).$$

The ToF velocity can be obtained by (8) and (9). Letting $\vec{v}_{\text{ToF}} = \vec{v}_{\text{Dop}}$, we can obtain $d_{t_m}^{(\text{spf})}$ and $d_{t_n}^{(\text{spf})}$ as specified in the proposition. ■

According to Proposition 1, given a pair of desired spoofing ToF distances $d_{t_m}^{(\text{spf})}$ and $d_{t_n}^{(\text{spf})}$ at time t_m and t_n, the attacker can calculate the required velocity that ensures a match between $\vec{v}_{\text{ToF}}$ and $\vec{v}_{\text{Dop}}$ by solving (12) and (13), so as to elude from being detected by the aforementioned detection mechanisms.

4) Spoofing Detection When Attacker Controls Its Velocity: A key insight of Proposition 1 is that the attacker's velocity must be coordinated with the ToF of the spoofing signals for a successful spoofing attack. Specifically, according to (12) and (13), given a pair of desired fake ToF distances and the victim LiDAR's velocity, the attacker's velocity $\vec{v}_a$ is fully determined. Therefore, when there exist two LiDARs of different velocities, both are scanning the attacker at the same time, then there is no way for the attacker to adjust its velocity to satisfy the requirements from both LiDARs—one key cannot open two locks. In this case, there will be at least one LiDAR, whose calculated ToF velocity is inconsistent with the Doppler velocity. Based on the above insight, we propose a cooperative LiDAR sensing scheme [28], [29], [30], [31] for our spoofing detection. A basic cooperative LiDAR system is shown in Fig. 10, which consists of two LiDARs: 1) a Coop-LiDAR and 2) an Ego-LiDAR. In cooperative LiDAR sensing, each LiDAR independently senses the environment and generates the data, and the generated sensing data are shared between them [30]. Note that in this scenario, it is essential to ensure the trustworthiness of the Cooperative LiDAR system, which can be guaranteed by using secured vehicle-to-vehicle (V2V) communication [32], [33], [34].

To detect the spoofing attack, we require LiDARs in the cooperative LiDAR system to move at different velocities. Each LiDAR computes its ToF velocity and Doppler velocity based on its received signals. The spoofing detection is conducted by checking whether the computed ToF velocity is consistent with the Doppler velocity at every LiDAR. To be more specific, suppose that we have N LiDARs in the cooperative LiDAR system with velocities $\vec{v}_L^{(1)}, \ldots, \vec{v}_L^{(N)}$, respectively. There exists at least a pair of LiDARs, say LiDAR i and LiDAR j, where $1 \leq i, j \leq N$, whose velocities are not equal, i.e., $|\vec{v}_L^{(i)}| \neq |\vec{v}_L^{(j)}|$. Each LiDAR calculates the Doppler velocity and the ToF velocity based on its received signals, which gives $\vec{v}_{\text{Dop}}^{(1)}$ and $\vec{v}_{\text{ToF}}^{(1)}, \ldots, \vec{v}_{\text{Dop}}^{(N)}$ and $\vec{v}_{\text{ToF}}^{(N)}$, respectively.

For legitimate signals, the ToF and Doppler velocities computed by each LiDAR are consistent, i.e., $\vec{v}_{\text{Dop}}^{(1)} = \vec{v}_{\text{ToF}}^{(1)} = \cdots = \vec{v}_{\text{Dop}}^{(N)} = \vec{v}_{\text{ToF}}^{(N)}$, because they all correspond to the velocity

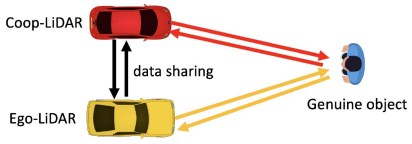


Fig. 10. Cooperative LiDARs.

of the same object. However, when a spoofing attacker is in place, it faces the following dilemma: on one hand, given the velocity of LiDAR i and the desired ToF distances to LiDAR i at time t_n and t_{n+1}, the attacker must set its velocity to, say $\vec{v}_a^{(i)}$, where $\vec{v}_a^{(i)}$ is decided based on Proposition 1, in order to elude from the detection of LiDAR i. On the other hand, given the velocity of LiDAR j and the desired ToF distances to LiDAR j at time t'_n and t'_{n+1}, where t'_n is close to t_n, and t'_{n+1} is close to t_{n+1}, the attacker must set its velocity to, say $\vec{v}_a^{(j)}$, where $\vec{v}_a^{(j)}$ is decided based on Proposition 1, in order to elude from the detection of LiDAR j. Because $|\vec{v}_L^{(i)}| \neq |\vec{v}_L^{(j)}|$, we can expect that in general $\vec{v}_a^{(i)} \neq \vec{v}_a^{(j)}$. Therefore, no matter which velocity the attacker chooses, at least one of LiDAR i and LiDAR j will be able to detect the attacker by testing the inconsistency between its calculated ToF velocity and Doppler velocity.

Alternatively, the attacker may just choose to move at velocity $\vec{v}_a^{(i)}$, and instead customize the spoofing ToF distances to LiDAR j at time t'_n and t'_{n+1} according to (12) and (13). In this way, the ToF velocity is consistent with the Doppler velocity at each of the LiDARs i and j, i.e., $\vec{v}_{\text{Dop}}^{(i)} = \vec{v}_{\text{ToF}}^{(i)}$ and $\vec{v}_{\text{Dop}}^{(j)} = \vec{v}_{\text{ToF}}^{(j)}$, however, it must be true that $\vec{v}_{\text{Dop}}^{(i)} \neq \vec{v}_{\text{Dop}}^{(j)}$. Therefore, by sharing their ToF velocities and Doppler velocities with each other, LiDARs i and j can also detect the spoofing attack based on the inconsistency between their respective Doppler velocities.

The proposed spoofing detection can be better illustrated by the following numerical examples. Without loss of generality, we use the 2-LiDAR cooperative LiDAR system shown in Fig. 10 as an example. The cooperative LiDAR system has one ego-LiDAR and one coop-LiDAR, and their velocities are denoted as $\vec{v}_L^{(\text{cop})}$ and $\vec{v}_L^{(\text{ego})}$, respectively. The Doppler velocities and ToF velocities computed by the two LiDARs for the same object are denoted as $\vec{v}_{\text{Dop}}^{(\text{cop})}$, $\vec{v}_{\text{ToF}}^{(\text{cop})}$ and $\vec{v}_{\text{Dop}}^{(\text{ego})}$, $\vec{v}_{\text{ToF}}^{(\text{ego})}$. For the attacker, denote its velocity by $\vec{v}_a = |\vec{v}_a|(\cos\phi_a, \sin\phi_a)$. The attacker sends spoofing signals $\mathbb{S}_{ego}^{(\text{spf})}$ and $\mathbb{S}_{\text{cop}}^{(\text{spf})}$ to ego-LiDAR and coop-LiDAR, respectively. And the ToF distances of $\mathbb{S}_{ego}^{(\text{spf})}$ and $\mathbb{S}_{\text{cop}}^{(\text{spf})}$ are designed according to Proposition 1 to maintain that for each LiDAR, the calculated Doppler velocity is consistent with the ToF velocity, i.e., $\vec{v}_{\text{Dop}}^{(\text{cop})} = \vec{v}_{\text{ToF}}^{(\text{cop})}$ and $\vec{v}_{\text{Dop}}^{(\text{ego})} = \vec{v}_{\text{ToF}}^{(\text{ego})}$.

The numerical results are shown in Fig. 11. In each subfigure, the x axis denotes $|\vec{v}_a|$, which varies from 0 to 20 m/s. The y axis represents the difference between the magnitudes of the two Doppler velocities, i.e., $|\vec{v}_{\text{Dop}}^{(\text{cop})}| - |\vec{v}_{\text{Dop}}^{(\text{ego})}|$. Recall that $\vec{v}_{\text{Dop}}^{(\text{cop})}$ and $\vec{v}_{\text{Dop}}^{(\text{ego})}$ are 2-D vectors, therefore if $|\vec{v}_{\text{Dop}}^{(\text{cop})}| - |\vec{v}_{\text{Dop}}^{(\text{ego})}| \neq 0$, then we must have $\vec{v}_{\text{Dop}}^{(\text{cop})} \neq \vec{v}_{\text{Dop}}^{(\text{ego})}$. We plot $|\vec{v}_{\text{Dop}}^{(\text{cop})}| - |\vec{v}_{\text{Dop}}^{(\text{ego})}|$ as functions of $|\vec{v}_a|$ in different combinations

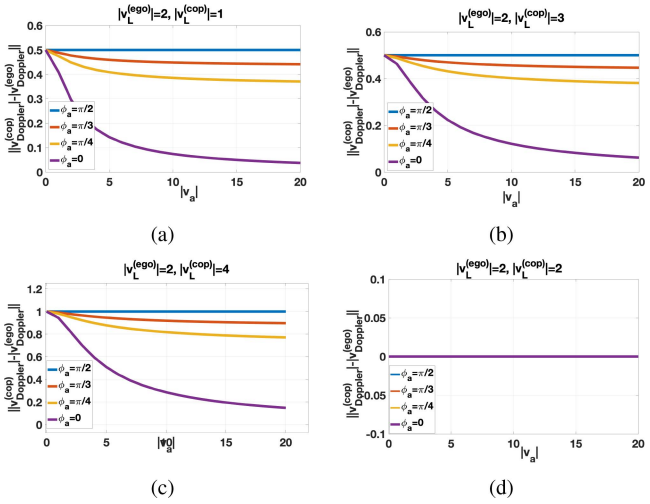


Fig. 11. Numerical examples for spoofing detection when attacker control its velocity. (a) $|v_L^{(ego)}| = 2, |v_L^{(cop)}| = 1$. (b) $|v_L^{(ego)}| = 2, |v_L^{(cop)}| = 3$. (c) $|v_L^{(ego)}| = 2, |v_L^{(cop)}| = 4$. (d) $|v_L^{(ego)}| = 2, |v_L^{(cop)}| = 2$.

of $|\vec{v}_L^{(\text{ego})}|$ and $|\vec{v}_L^{(\text{cop})}|$ in the four subfigures: (a) $|\vec{v}_L^{(\text{ego})}| = 2$ m/s, $|\vec{v}_L^{(\text{cop})}| = 1$ m/s, (b) $|\vec{v}_L^{(\text{ego})}| = 2$ m/s, $|\vec{v}_L^{(\text{cop})}| = 3$ m/s. (c) $|\vec{v}_L^{(\text{ego})}| = 2$ m/s, $|\vec{v}_L^{(\text{cop})}| = 4$ m/s, and (d) $|\vec{v}_L^{(\text{ego})}| = 2$ m/s, $|\vec{v}_L^{(\text{cop})}| = 2$ m/s. In each subfigure, we also vary the angle of the attacker's velocity, i.e., ϕ_a, by setting $\phi_a = (\pi/2), (\pi/3), (\pi/4), 0$, respectively.

In Fig. 11(a)–(c), the two LiDARs in the cooperative LiDAR system have different velocity magnitudes, i.e., $|\vec{v}_L^{(\text{ego})}| \neq |\vec{v}_L^{(\text{cop})}|$. Although the spoofing attack maintains that the ToF velocity is consistent with the Doppler velocity at each of LiDARs ($\vec{v}_{\text{Dop}}^{(\text{cop})} = \vec{v}_{\text{ToF}}^{(\text{cop})}$ and $\vec{v}_{\text{Dop}}^{(\text{ego})} = \vec{v}_{\text{ToF}}^{(\text{ego})}$), when the Doppler velocities are shared in the cooperative LiDAR system, ego-LiDAR and coop-LiDAR can detect spoofing attacks because $\vec{v}_{\text{Dop}}^{(\text{cop})} \neq \vec{v}_{\text{Dop}}^{(\text{ego})}$ ($|\vec{v}_{\text{Dop}}^{(\text{cop})}| - |\vec{v}_{\text{Dop}}^{(\text{ego})}| \neq 0$). A special case is shown in Fig. 11(d), when the two LiDARs have the same velocity magnitude, that is, $|\vec{v}_L^{(\text{cop})}| = |\vec{v}_L^{(\text{ego})}|$, we have $|\vec{v}_L^{(\text{cop})}| - |\vec{v}_L^{(\text{ego})}| = 0$ even when the spoofing attack is in place. In this case, the cooperative LiDAR system cannot detect spoofing attacks based on the inconsistency between their respective Doppler velocities. Therefore, our spoofing detection scheme requires that the LiDARs in the cooperative LiDAR system have different velocities to successfully detect the spoofing attack.

C. Attack Model 3 (Moving Attacker That Controls Both Its Velocity and Signal Frequency)

A basic assumption in Attack Models 1 and 2 is that the attacker transmits spoofing signals of the same frequency as that of the victim LiDAR and it does not manipulate the frequency of the spoofing signal during the attack. Although this assumption is valid for many spoofing attack scenarios and has been adopted by many existing studies, e.g., [7], [8], and [35], an attacker may use frequency modulation or a tunable laser source to dynamically change the frequency of the spoofing signal, so as to create a faked Doppler frequency shift to mislead those spoofing detection

mechanisms proposed in the previous sections. This is elaborated as follows.

1) Spoofing Attack in Attack Model 3: When an attacker can dynamically adjust the frequency of the spoofing signal, besides sending spoofing ToF signals to the victim LiDAR, the attacker also compensates for the frequency offset caused by the Doppler effect by changing the frequency of the transmitted spoofing signal, making the frequency offset of the spoofing signal received by the victim LiDAR identical to the Doppler frequency shift of the legitimate signal.

Specifically, let us consider a typical spoofing attack scenario, where at the current moment the distance between the (victim) LiDAR and the attacker is d. The relative radial velocity between the victim LiDAR and the attacker is $\Delta v_a = (\vec{v}_L - \vec{v}_a) \cdot \vec{l}$, where $\vec{l}$ is the unit vector along the direction from the LiDAR to the attacker. The goal of the attacker is to create a fake object that is d' away from the LiDAR, in the same direction of $\vec{l}$ (so the LiDAR, the attacker, and the fake object are collinear) and of a relative radial velocity of Δv_{spoof}, where $\Delta v_{\text{spoof}} = (\vec{v}_L - \vec{v}_{\text{spoof}}) \cdot \vec{l}$, and $\vec{v}_{\text{spoof}}$ denotes the velocity of the fake object. With time continues, the trajectory of the faked object (i.e., d's) should be consistent with $\vec{v}_{\text{spoof}}$.

To achieve the attack goal, in the time domain, the attacker sends spoofing signals with faked ToF distance of d'. In the frequency domain, the attacker adjusts the frequency of the transmitted spoofing signal to mimic the Doppler shift experienced by a legitimate signal. Specifically, if a genuine object of velocity $\vec{v}_{\text{spoof}}$ is at the location of the fake object, then the Doppler shift experienced by a legitimate signal (this is the signal sent out by the LiDAR, reflected by the object, and then received by the LiDAR) is given by $\Delta f_r = (2f_0/c)\Delta v_{\text{spoof}}$, where f_0 is the frequency of the transmitted (legitimate) signal. Therefore, the frequency of the received legitimate signal is given by $f_0 + \Delta f_r$. To mimic the legitimate signal, the attacker chooses a frequency f_a for the transmitted spoofing signal, such that when the spoofing signal is received by the victim LiDAR, the frequency of the received spoofing signal is identical to that of the received legitimate signal. Since the spoofing signal is sent directly to the LiDAR, its Doppler shift is given by $\Delta f_a = (f_a/c)\Delta v_a$. So the frequency of the received spoofing signal is $f_a + \Delta f_a$. Therefore, the f_a that satisfies the aforementioned requirement is given by

$$f_a = \frac{c + 2\Delta v_{\text{spoof}}}{c + \Delta v_a} f_0. \tag{15}$$

In this way, the Doppler shift measured by the victim LiDAR happens to be Δf_r. As a result, the calculated Doppler velocity is consistent with the ToF velocity (both are equivalent to $\vec{v}_{\text{spoof}}$), and hence the fake object will be accepted by the LiDAR as a genuine one.

2) Spoofing Detection When Attacker Controls Signal Frequency: The cooperative LiDAR system can also be used for spoofing detection when the attacker controls its signal frequency. Specifically, according to (15), the attacker must adjust the frequency of the transmitted signal each time when sending a spoofing signal to a LiDAR. When there exist multiple LiDARs with different velocities (so they have different Δv_a's and Δv_{spoof}'s), the attacker must choose different transmission frequencies when sending to different LiDARs to spoof each of them.

Based on this observation, we can use the cooperative LiDAR system and require all LiDARs in the system be synchronized to send probing laser pulses that will hit the object at the same time (and hence will be reflected by the object at the same time too), so that an attacker is not able to simultaneously change the frequency of spoofing signals for all LiDARs at once. The key point in achieving full synchronization among a group of cooperative LiDARs, i.e., making them point to the same object at the same time, is to realize that the first LiDAR that detects the object actually can compute and then communicate the location of that object to all other collalborating LiDARs, and hence allow all LiDARs in the group to compute their respective angles of departure for their laser beams in order for them to point to the same object.

The basic idea of using multiple LiDARs for spoofing detection is that an attacker can only send out a spoofing signal with a certain frequency at one time. Given that our Coop-LiDAR system synchronizes multiple LiDARs to monitor the same object at the same time, it is hard for an attacker to send a single spoofing signal that can simultaneously satisfy the frequency requirements from all LiDARs. In the case where the attacker has k coordinated dynamic-frequency laser transmitters, at least $k+1$ synchronized LiDARs are needed, so that at least one LiDAR is able to detect the spoofing by testing the inconsistency between its calculated Doppler velocity and ToF velocity. Note that here, the goal of the spoofing detection mechanism is to serve as a filter (a gate-keeper) that identifies and rejects spoofed LiDAR sensing outcomes. Therefore, a collective decision-making process is adopted among all $(k+1)$ LiDARs: a sensed point in the point cloud will be accepted only if none of the $k+1$ synchronized LiDARs has a negative detection outcome.

D. Limitations

Although in previous sections we have demonstrated that the Doppler-shift-based method is effective for detecting spoofing attacks across various real-world attack scenarios, there still remain some scenarios where our method may be less effective or not suitable, as elaborated below.

1) *Static or Low-Relative Velocities Scenarios:* Doppler shift is the change of signal frequency due to the movement of the transmitter in relative to the receiver. In the LiDAR case, if the relative velocity between the LiDAR and the sensed object is 0 or close to 0, then the Doppler shift will be negligible. In these scenarios, our method is not applicable.
2) *Large Velocity Variation During Small Time Interval Scenarios:* A basic assumption in our attack models 2 and 3 is that the relative velocity between the LiDAR and the object remains constant between the moments of two consecutive LiDAR measurements (usually this is over the span of a fraction of a second), so that our proposed algorithm is able to resolve the Doppler velocity and the ToF velocity of the object. While this assumption is

valid in most cases, in reality there are special situations where the relative velocity between the LiDAR and the object changes significantly during the aforementioned small interval. Such changes in velocity could be caused by, e.g., a bumpy road condition, or a complicated traffic condition that requires frequent maneuvers (e.g., sudden acceleration, deceleration, or braking) of the car. In these special situations, the accuracy of the proposed method will be reduced. To deal with this issue, in Section VI, we have proposed a statistical spoofing detection scheme, which accounts for the short-term variation/perturbation in the vehicle's velocity. However, the proposed statistical detection scheme still faces limitations as it is based on certain assumed statistical models (i.e., the distribution) for the velocity variation. In the real-world scenario, if the actual velocity variation deviates significantly from the assumed distribution, then the accuracy of this statistical scheme will be reduced. In this case, a combination of our method with existing model-level defense methods would be a good solution. As model-level defense methods utilize high-level contextual relationships between multiple data points for spoofing detection, they well compensate for the limitations of the Doppler shift-based method that works only at the physical layer.

We want to clarify that our proposed spoofing detection method is not a panacea - a "solution to all" that intends to replace existing methods. Instead, it serves as the "first line of defense" that operates in the signal space and is designed to complement existing model-level defense methods. Our method uses the physical property of an individual data point within the point cloud for spoofing attack detection, which is a validation in the signal space to check whether the signatures (Doppler shift) of the signal follow physical principles. Because of its physical feature, our proposed method can fundamentally ensure that the LiDAR sensing results that are fed to the subsequent high-level processing are authentic. In contrast, current perception models-level defense methods work at a higher level: they first aggregate multiple data points to establish a geometric representation for the sensed object, and then examine whether this geometric representation presents a reasonable contextual consistency over time. It is clear that our method works in an orthogonal space compared to these model-level defense methods. In practice, both methods can be applied at the same time to improve the overall detection accuracy against LiDAR spoofing attacks.

VI. Spoofing Detection With Joint Consideration of Velocity and Acceleration

In the previous section, we assumed a uniform motion model, so that the relative velocity between the LiDAR and the object can be seen as constant. And we propose to verify the consistency between the ToF velocity and the Doppler velocity for spoofing attack detection. Although, due to the high-scanning rate of LiDAR, the motion of an object with acceleration can be seen as a uniform motion, the presence of acceleration introduces additional variance in velocity estimation, which makes spoofing detection based only on velocity unreliable.

In this section, we present a hypothesis-test-based spoofing detection framework that jointly considers velocity and acceleration. We first formulate the hypotheses for the attack and nonattack cases on the basis of our previous findings. Then, we demonstrate the necessity to jointly consider acceleration and velocity for spoofing detection and provide the test statistic designing strategies. Finally, we perform power analysis under various conditions and numerically determine the smallest test sample size required to achieve an expected performance level.

A. Hypothesis Test Formulation

According to our discussion in the previous section, the velocity of an object can be obtained based on the Doppler shift or ToF of the received signal, namely, $\vec{v}_{\text{Dop}}$ and $\vec{v}_{\text{ToF}}$. The inconsistency between the two velocities, $\vec{v}_{\text{Dop}}$ and $\vec{v}_{\text{ToF}}$, can only be caused by spoofing attacks or noise. Consider a sequence of n Doppler and ToF velocity samples $\{\vec{v}_{\text{Dop}}\}_n$ and $\{\vec{v}_{\text{ToF}}\}_n$, respectively. For convenience, let v_{Dop} and v_{ToF} denote the magnitudes of $\vec{v}_{\text{Dop}}$ and $\vec{v}_{\text{ToF}}$, respectively. And their population means are denoted by μ_{Dop} and μ_{ToF}, respectively. The spoofing detection can be formulated as a hypothesis test, which essentially tests whether the two means are equal or not, that is, $\mu_{\text{Dop}} \stackrel{?}{=} \mu_{\text{ToF}}$. The null and alternative hypotheses can be formulated as follows:

$$\begin{aligned} \mathcal{H}_0&: \text{ no spoofing attack.}(\mu_{\text{Dop}} = \mu_{\text{ToF}}) \\ \mathcal{H}_a&: \text{ the presence of a spoofing attack.}(\mu_{\text{Dop}} \neq \mu_{\text{ToF}}). \end{aligned} \tag{16}$$

When only velocity is taken into account for spoofing detection, the two-sample t-test is used. The test statistic is calculated as

$$t = \frac{|\mu_{\text{Dop}} - \mu_{\text{ToF}}|}{S_{\text{pooled}}\sqrt{2/n}} \tag{17}$$

where $S_{\text{pooled}} = ([s_1^2 + s_2^2]/2)$, and s_1^2 and s_2^2 are the sample variances of v_{Dop} and v_{ToF}, respectively.

Then t is compared with the critical value with the degree of freedom of $n-1$ and the significance level α, $t_{n-1}(\alpha/2)$. Hypothesis $\mathcal{H}_0$ is rejected if $t > t_{n-1}(\alpha/2)$, which indicates a spoofing attack.

B. Joint Consideration of Velocity and Acceleration

In real driving scenarios, the AV's motion not only has velocity but also has acceleration. Such an acceleration could lead to a broadening spectrum in the Doppler frequency, which increases the variance in velocity estimations derived from the Doppler shift spectrum. This variance becomes more significant for the small velocity and large acceleration cases. For example, suppose that we have $v = 0.5$ m/s and $a = 0.5$ m/s^2, the Doppler spectrum of the received signals is likely to display two dominant peaks at velocities of 0.5 m/s and 1 m/s. This phenomenon can lead to ambiguity in velocity estimation, with potential values ranging between 0.5 m/s or 1 m/s, thus introducing a maximal error of 0.5 m/s. Hence, when acceleration exists, it increases the

risk of misidentifying a legitimate signal as a spoofing attack, resulting in an increased false alarm rate in spoofing attack detection. Realizing the limitation of considering velocity alone in spoofing attack detection, we introduce an advanced detection mechanism that jointly incorporates the effect of both velocity and acceleration, which can provide more robust and accurate results in identifying spoofing attacks in realistic driving scenarios.

Let a denote the acceleration and let $\boldsymbol{x} = [v, a]$ denote the multivariate variable that consists of both the velocity v and the acceleration a, which is used for the hypothesis test. We first use maximum likelihood estimation (MLE) to estimate v_{ToF} and a_{ToF}. Let $\boldsymbol{\mu}_{\text{Dop}}$, $\boldsymbol{\Sigma}_{\text{Dop}}$ and $\boldsymbol{\mu}_{\text{ToF}}$, $\boldsymbol{\Sigma}_{\text{ToF}}$ denote the mean and variance of the population for $\bar{\boldsymbol{x}}_{\textbf{Dop}}$ and $\bar{\boldsymbol{x}}_{\text{ToF}}$, respectively. We assume that $\{\boldsymbol{x}_{\text{Dop}}\}_n$ is a random sample of size n from the normal distribution $\mathcal{N}(\boldsymbol{\mu}_{\text{Dop}}, \boldsymbol{\Sigma}_{\text{Dop}})$ and $\{\boldsymbol{x}_{\text{ToF}}\}_n$ is a random sample of size n from normal distribution $\mathcal{N}(\boldsymbol{\mu}_{\text{ToF}}, \boldsymbol{\Sigma}_{\text{ToF}})$. Note that $\bar{\boldsymbol{x}}_{\text{Dop}} - \bar{\boldsymbol{x}}_{\text{ToF}}$ follows the normal distribution $\mathcal{N}(\boldsymbol{\mu}_{\text{Dop}} - \boldsymbol{\mu}_{\text{ToF}}, (1/n)(\boldsymbol{\Sigma}_{\text{Dop}} + \boldsymbol{\Sigma}_{\text{ToF}}))$. Therefore, the hypothesis test is simplified accordingly to test if $\boldsymbol{\mu}_{\text{Dop}} = \boldsymbol{\mu}_{\text{ToF}}$ or not, and *Hotelling's* T^2 test is used, whose test statistic is

$$T_0^2 = [\bar{\boldsymbol{x}}_{\text{Dop}} - \bar{\boldsymbol{x}}_{\text{ToF}} - (\boldsymbol{\mu}_{\text{Dop}} - \boldsymbol{\mu}_{\text{ToF}})]'[\frac{2}{n} S_{\text{pooled}}]^{-1} [\bar{\boldsymbol{x}}_{\text{Dop}} - \bar{\boldsymbol{x}}_{\text{ToF}} - (\boldsymbol{\mu}_{\text{Dop}} - \boldsymbol{\mu}_{\text{ToF}})] \tag{18}$$

where $S_{\text{pooled}} = ([s_1^2 + s_2^2]/2)$, and $\bar{\boldsymbol{x}}_{\text{Dop}}$ and $\bar{\boldsymbol{x}}_{\text{ToF}}$, and s_1^2 and s_2^2 are the sample mean and sample variance of $\boldsymbol{x}_{\text{Dop}}$ and $\boldsymbol{x}_{\text{ToF}}$, respectively. T_0^2 follows a noncentral F distribution $(4n - 4/2n - 3)F_{2,2n-3}$. For a given significance level α, the critical value τ is calculated as

$$\tau = \frac{4n-4}{2n-3} F_{2,2n-3}(\alpha). \tag{19}$$

The null hypothesis $\mathcal{H}_0$ is rejected when $T_0^2 > \tau$, and the false alarm rate, a.k.a., type I error, is

$$P_{\mathcal{H}_0}(T_0^2 > \tau) = \alpha. \tag{20}$$

C. Formulation of $\mathcal{H}_a$ for Power Analysis

Fig. 12 illustrates the power and significance level of a statistical test. Previously, we have determined the distribution of $\mathcal{H}_0$ and the critical value. Next, we must ensure that the test has enough power so that the distribution of $\mathcal{H}_0$ and that of $\mathcal{H}_a$ are sufficiently apart and both type I and type II errors are small. The power of a hypothesis test is the probability that the test correctly rejects the null hypothesis, as illustrated by the red dashed area. It should be noted that statistical power is positively related to the sample size. The larger the sample size, the easier it is to achieve the expected statistical power. There are two possible cases where one fails to reject the null hypothesis: 1) the null hypothesis is really true and 2) the sample size is not large enough to reject the null hypothesis (i.e., statistical power is too low). Additional samples may be needed to either accept or reject the null hypothesis.

Now, we will design scenarios of $\mathcal{H}_a$, under which the power analysis can be performed to determine the smallest sample size required to achieve a satisfactory detection

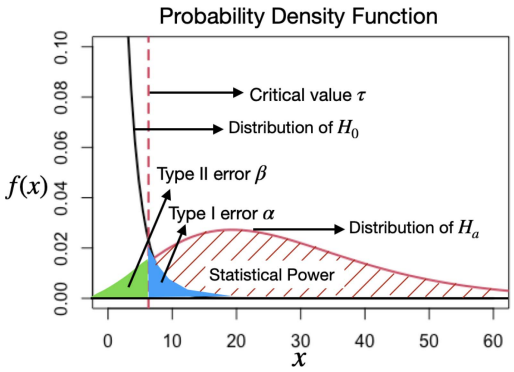


Fig. 12. Illustration of a statistical test.

performance. When designing $\mathcal{H}_a$, it is impossible to enumerate all possibilities. In fact, the detector is not designed to identify every malicious attack, but rather to identify spoofing attacks that can lead to severe consequences. Specifically, in our study, we focus on two attack goals: 1) *emergency brake* triggered by injecting a fake static object in front of the LiDAR and 2) *failure of the automatic braking system* by injecting a fake object that is relatively stationary to the LiDAR. Specifically, we consider a scenario where the AV is fast-moving toward a static real obstacle, and a brake decision is required to avoid a collision. Note that the braking decision of the AV system is based on the combination consideration of the distance and the relative speed between the AV and the object. Therefore, the attacker launches the attack by sending spoofing signals that mimic a fake object in close range (so the faked signal will be the first to arrive at the AV's LiDAR than that of the real object) to hide the real obstacle from LiDAR detection and is relatively stationary to the AV. Although the distance between the fake object and the AV is small, due to the small relative speed between them, the AV's decision-making system will not trigger a braking decision, as it perceives no immediate collision risk. Consequently, the AV might continue at its current speed and collide with the real obstacle. In addition to the above attack goals, we also consider the attacker to be static or mobile and design three attack scenarios, in which we provide the distribution of $\mathcal{H}_a$.

1) Attack Scenario 1 (Emergency Brake Triggered by Static Attacker): A static attacker wants to trigger an emergency brake by faking a static object in front of the LiDAR. Because both the attacker and the fake object are static, according to (5) and (6), we have $\mathcal{H}_a$: $\boldsymbol{\mu}_{\text{Dop}} = 2\boldsymbol{\mu}_{\text{ToF}}$. The test statistic under $\mathcal{H}_a$ is

$$T_a^2 = [\bar{\boldsymbol{x}}_{\text{Dop}} - 2\bar{\boldsymbol{x}}_{\text{ToF}} - (\boldsymbol{\mu}_{\text{Dop}} - 2\boldsymbol{\mu}_{\text{ToF}})]'[\frac{5}{n} S_{\text{pooled}}]^{-1} [\bar{\boldsymbol{x}}_{\text{Dop}} - 2\bar{\boldsymbol{x}}_{\text{ToF}} - (\boldsymbol{\mu}_{\text{Dop}} - 2\boldsymbol{\mu}_{\text{ToF}})]. \tag{21}$$

According to [36], the test statistic T_a^2 follows a noncentral F distribution $[25(n-1)/5n-6]F_{2,5n-6}$ with a *noncentrality parameter* (*n.c.p.*) equal to

$$n.c.p. = \frac{n}{\sigma^2}\left[(\bar{\boldsymbol{x}}_{\text{Dop}} - \bar{\boldsymbol{\mu}})'(\bar{\boldsymbol{x}}_{\text{Dop}} - \bar{\boldsymbol{\mu}}) + (2\bar{\boldsymbol{x}}_{\text{ToF}} - \bar{\boldsymbol{\mu}})'(2\bar{\boldsymbol{x}}_{\text{ToF}} - \bar{\boldsymbol{\mu}})\right] \tag{22}$$

where $\bar{\boldsymbol{\mu}} = [(2\boldsymbol{\mu}_{\text{Dop}} + \boldsymbol{\mu}_{\text{ToF}})/2]$ and σ^2 is the mean square error. Given a critical value τ, the type II error is represented as

$$P_{\mathcal{H}_a}(T_a^2 < \tau) = \beta. \tag{23}$$

2) Attack Scenario 2 (Emergency Brake Triggered by Moving Attacker): The attacker is moving at the same speed as the victim LiDAR and wants to trigger an emergency brake by faking a static object in front of the victim LiDAR. In this case, we have $\mathcal{H}_a$: $\boldsymbol{\mu}_{\text{Dop}} = 0$ and $\boldsymbol{\mu}_{\text{ToF}} \neq 0$. The test statistic under $\mathcal{H}_a$ is

$$T_a^2 = [\bar{\boldsymbol{x}}_{\text{Dop}} - \bar{\boldsymbol{x}}_{\text{ToF}} + \boldsymbol{\mu}_{\text{ToF}})]' \left[\frac{2}{n} S_{\text{pooled}}\right]^{-1} [\bar{\boldsymbol{x}}_{\text{Dop}} - \bar{\boldsymbol{x}}_{\text{ToF}} + \boldsymbol{\mu}_{\text{ToF}})] \tag{24}$$

$$\text{with } n.c.p. = \frac{n}{\sigma^2}[(\bar{\boldsymbol{x}}_{\text{Dop}} - \boldsymbol{\mu}_{\text{ToF}})'(\bar{\boldsymbol{x}}_{\text{Dop}} - \boldsymbol{\mu}_{\text{ToF}}) + (\bar{\boldsymbol{x}}_{\text{ToF}} - \boldsymbol{\mu}_{\text{ToF}})'(\bar{\boldsymbol{x}}_{\text{ToF}} - \boldsymbol{\mu}_{\text{ToF}})] \tag{25}$$

which follows $(4n - 4/2n - 3)F_{2,2n-3}$.

3) Attack Scenario 3 (Failure of Automatic Braking System Triggered by Static Attacker): The attacker is static and wants to trigger a failure of the automatic braking system of an AV. The attacker sends spoofing signals that mimic a fake object in close range and is relatively stationary to the AV. In this case, we have $\mathcal{H}_a$: $\boldsymbol{\mu}_{\text{Dop}} \neq 0$ and $\boldsymbol{\mu}_{\text{ToF}} = 0$. The test statistic under $\mathcal{H}_a$ is

$$T_a^2 = [\bar{\boldsymbol{x}}_{\text{Dop}} - \bar{\boldsymbol{x}}_{\text{ToF}} - \boldsymbol{\mu}_{\text{Dop}})]' \left[\frac{2}{n} S_{\text{pooled}}\right]^{-1} [\bar{\boldsymbol{x}}_{\text{Dop}} - \bar{\boldsymbol{x}}_{\text{ToF}} - \boldsymbol{\mu}_{\text{Dop}})] \tag{26}$$

$$\text{with } n.c.p. = \frac{n}{\sigma^2}\left[(\bar{\boldsymbol{x}}_{\text{Dop}} - \boldsymbol{\mu}_{\text{Dop}})'(\bar{\boldsymbol{x}}_{\text{Dop}} - \boldsymbol{\mu}_{\text{Dop}}) + (\bar{\boldsymbol{x}}_{\text{ToF}} - \boldsymbol{\mu}_{\text{Dop}})'(\bar{\boldsymbol{x}}_{\text{ToF}} - \boldsymbol{\mu}_{\text{Dop}})\right] \tag{27}$$

which follows $(4n - 4/2n - 3)F_{2,2n-3}$.

D. Settings for Power Analysis

As mentioned above, the sample size should be large enough to provide the expected statistical power. As a result, both the type I error α from $P_{\mathcal{H}_0}(T_0^2 > \tau) = \alpha$ and the type II error from $P_{\mathcal{H}_a}(T_a^2 < \tau) = \beta$ are controlled in acceptable ranges. Analysis is carried out in combinations of road conditions, spoofed signal proportion, signal SNR, and attack scenarios to determine the minimum sample size required for the detector to produce satisfactory results for the most practical $\boldsymbol{x}$.

1) Road Condition: Three typical road conditions are considered: 1) highway driving ($v = 33$ m/s and $a = 0.5$ m/s^2); 2) ramp driving ($v = 20$ m/s and $a = 1.5$ m/s^2); and 3) city driving ($v = 11$ m/s and $a = 5$ m/s^2). We note that the relative speed implies the distance between the LiDAR and the object. A low-relative speed indicates a smooth driving condition, under which any attack can be easily detected due to the sudden change in speed measurements. Rather, a high-relative speed may indicate that an abnormal traffic condition is already in place, making the attack less effective. Therefore, we set the relative speed of the victim LiDAR to be 50% of that of each road condition to balance between the difficulty of detection and the consequence of the attack.

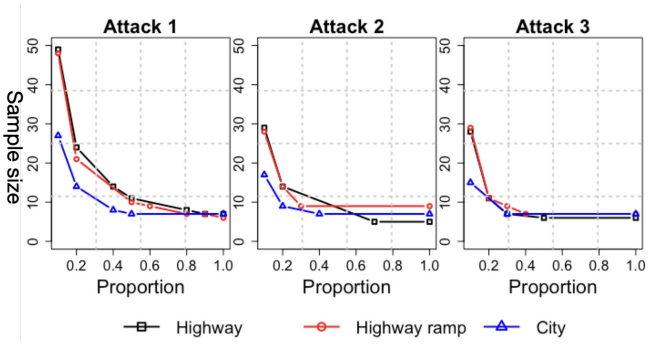


Fig. 13. Number of samples needed for each road conditions under different spoofed signal proportion.

2) Spoofed Signal Proportion: The high-LiDAR sampling rate and the narrow receiver's field-of-view impose stringent constraints on the timing and direction of the spoofed signal. In practice, the attacker hardly has the luxury of continuously spoofing a sequence of signals [23], [37]. It is more practical that the attacker spoofs the LiDAR signals intermittently. The spoofed signal proportion is defined as the ratio of the number of spoofing signal samples to the number of received signal samples. The higher the ratio of the spoofed signal, the easier the attack is detected. In the experiment, we consider the range of the proportion of the spoofed signal p to be 0.1 to 1.

3) Signal-to-Noise Ratio: The noise level of the signals is affected by weather conditions, ambient light, system error, device noise, etc. Such noises would introduce errors in the velocity estimated from both the ToF and Doppler shift, and we discuss them separately. Considering the LiDAR measurement error [38] and the disturbance of ambient light, we set the error rate of both a_{ToF} and v_{ToF} to 3%. For the measurement error in Doppler velocity, we follow [39] to calculate the variance of $\boldsymbol{x}_{\text{Dop}}$ of MLE

$$\sigma_v^2 = \frac{1}{\text{SNR}} \frac{3}{2\pi^2 N^2}, \sigma_a^2 = \frac{1}{\text{SNR}} \frac{45}{2\pi^2 N^4} \tag{28}$$

where N is the sampling length of the signal, which is set to 256 in our simulation to tradeoff the estimation accuracy and the system burden. The SNR is set to $\{10^{-6}, 10^{-5}, 10^{-4}\}$ according to [16] to fit the real-world scenarios.

E. Numerical Results of Power Analysis

In our simulation, we follow the convention to set the type I error to $\alpha = 0.05$, and record the least number of samples to achieve the power of 0.9 at each $\mathcal{H}_a$, i.e., type II error is $\beta = 0.1$. The $F1$ score in this setting is 0.923, indicating satisfactory spoofing detection performance. In real-world application scenarios, the type I and type II error settings can be set differently to meet different practical requirements.

1) Impact of Spoofing Signal Proportion: We set the SNR to 10^{-4} and vary the proportion of the spoofed signal from 0.1 to 1. We record the least number of samples needed to achieve the preset significance level under different attack scenarios and road conditions. The results are shown in Fig. 13. It can be seen that more samples are needed when the proportion

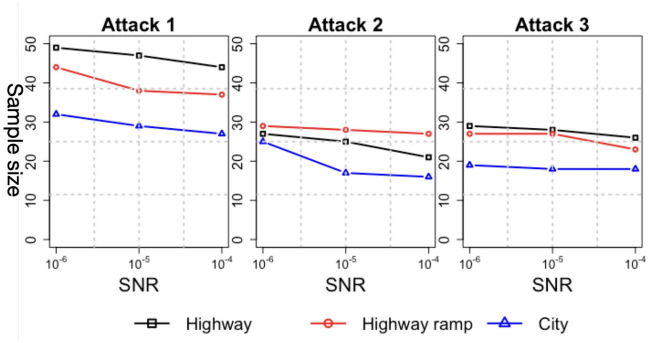


Fig. 14. Number of samples needed for each road conditions under different SNR.

of the spoofed signal is small. When the attacker spoofs only a small proportion of the LiDAR signals, the mean of $\boldsymbol{x}_{\text{ToF}}$ is close to that of $\boldsymbol{x}_{\text{Dop}}$, therefore, more samples are needed to separate the two distributions. This phenomenon becomes more obvious when the proportion of the spoofed signal is less than 40%, especially for attack 1.

2) Impact of Signal-to-Noise Ratio: Then, we fix the proportion of the spoofed signal to 0.1 and vary the SNR from 10^{-6} to 10^{-4}. The minimal sample sizes needed to provide the expected statistical power under various attack scenarios and road conditions are shown in Fig. 14. Compared to the spoofed signal proportion that has a greater impact on the difference between the means of $\{\boldsymbol{x}_{\text{ToF}}\}_n$ and $\{\boldsymbol{x}_{\text{Dop}}\}_n$, the SNR plays a more significant role in affecting their variance. A smaller SNR leads to a larger estimation variance in the velocity and acceleration from the Doppler shift, which increases the uncertainty in detecting spoofing attacks. As a result, more test samples are needed to provide sufficient statistical power.

F. Discussion on Implementation

After determining the number of samples required, the spoofing attack detection procedure is carried out in the following two steps.

1) *Data Collection:* Assuming that the sample size is 50, 50 samples of $\{\boldsymbol{x}_{\text{dop}}\}$ and $\{\boldsymbol{x}_{\text{ToF}}\}$ are collected, respectively.
2) *Testing:* The test statistic is calculated according to (18), then compared with the threshold τ predefined by (19).

If the test statistic is greater than the threshold, it suggests the potential presence of a spoofing attack. According to the analysis above, setting the sample size to 50 is sufficient for our test to achieve an $F1$ score of 0.923 in the worst-case scenario. Notably, with sample size of 50, the $F1$-score would be even higher for the remaining cases. For example, under conditions where 40% of the signals are spoofed and the SNR is 10^{-4}, the test produces an impressive $F1$ score of 0.97 in all road conditions.

We then evaluate the time complexity of the proposed method by examining the latency associated with each step above. In the testing step, the calculation of the test statistic directly from the data and the comparison with the predefined threshold incurs negligible time overhead. In the data collection phase, considering a typical 16-beam Velodyne LiDAR system with a rotation speed of 20 Hz [40], 50 samples can be collected in 150 ms. This duration is significantly shorter than the average reaction time of 830 ms for AVs [41]. Note that for more advanced AV LiDAR systems with a higher number of laser beams and a faster rotation speed, the data collection time can be further reduced. As a result, our proposed spoofing attack detection mechanism can operate simultaneously with established LiDAR processing algorithms, enhancing the reliability of current AV driving systems without introducing additional time overhead.

VII. Applicability Discussion, Future Works, and Conclusion

A. Applicability Discussion

In this section, we discuss the applicability of the proposed method to other sensors, such as cameras and radars. The primary focus of this article is on addressing the unique problem of safeguarding against LiDAR spoofing attacks, which is distinctive due to the special way of how a LiDAR sensor detects an object and its distance to that object. Therefore, our proposed method cannot be applied to cameras, as cameras lack the capability to measure the Doppler shift of incoming light signals. Specifically, cameras are passive sensors that record natural radiation either emitted or reflected from objects. The resulting signal is represented in terms of pixel intensity and color, and cameras cannot capture any frequency changes in these light signals. As for radars, our proposed method can be used for spoofing attack detection but requires adaptations to address the challenges inherent to radar systems. Notably, while radars are also active sensors and can directly measure the Doppler shift of incoming signals, they present unique challenges when compared to LiDARs. For example, radars typically offer lower spatial resolution and emit signals with a larger spectral bandwidth. This means that the received signal can be influenced by the Doppler effect from several objects simultaneously, each contributing different Doppler frequency shift components. Additionally, the broad spectral bandwidth of radar signals can reduce the precision of Doppler frequency shift measurements. This complexity heightens the challenge of pinpointing spoofing attacks-based solely on the Doppler shift and potentially increasing the false positive rate of our proposed method when being applied to radars.

B. Future Work

We understand that testing our method in a real-world setup, such as on a real AV, would significantly improve the impact and practical relevance of our method. However, as a research lab in a university, we are not capable of fully implementing the proposed methods on a real LiDAR system (note that nearly all LiDAR systems on the market are proprietary and are not open to redevelopment) and then mounting it on a vehicle to perform real-world testing. Realistically, what our capacity allows us to do is the theoretical study of the mathematical models for the spoofing attacks and their detection, and mainly computer-simulation-based performance evaluation for the proposed models. The scope of this article has to be decided by our capacity above. We acknowledge that

there must exist a significant difference between our work and a real-world system that can be directly used by the current autonomous driving vehicles. However, our contribution in this article is mainly on the modeling aspect of the problem rather than on the system-building/implementation of the model. The theoretical foundation laid in this work could serve as an important reference/guideline for system implementation in the next step, which is out of the scope of this article and may be conducted in our future work.

C. Conclusion

In this article, we investigated the LiDAR security problem in the autonomous driving system. We performed a detailed analysis on the vulnerability of the LiDAR sensors. To better illustrate how to use Doppler shift for spoofing attack detection in different attack scenarios, we considered three attack models, including static attacker, moving attacker without/with control of velocity, and moving attacker with control of both velocity and signal frequency. Under each of these models, we first show how the spoofing attack is performed, and then present our proposed countermeasures. To address the uncertainty caused by vehicle acceleration, we proposed a statistical spoofing detection framework to jointly consider the impact of acceleration on vehicle velocity. Extensive numerical evaluations are conducted to verify the effectiveness and accuracy of the proposed methods in a wide range of test settings.

ACKNOWLEDGMENT

Any opinions, findings, conclusions, or recommendations expressed in this article are those of the author(s) and do not necessarily reflect the views of NSF.

REFERENCES

[1] J. Cui, X. Chen, J. Zhang, Q. Zhang, and H. Zhong, "Toward achieving fine-grained access control of data in connected and autonomous vehicles," *IEEE Internet Things J.*, vol. 8, no. 10, pp. 7925–7937, May 2021.

[2] J. Van Brummelen, M. O'Brien, D. Gruyer, and H. Najjaran, "Autonomous vehicle perception: The technology of today and tomorrow," *Transp. Res. C, Emerg. Technol.*, vol. 89, pp. 384–406, Apr. 2018.

[3] Waymo, Mountain View, CA, USA. "Waymo driver." May 2009. [Online]. Available: https://waymo.com/intl/zh-cn/waymo-driver/

[4] S. Li, S. Wang, Y. Zhou, Z. Shen, and X. Li, "Tightly coupled integration of GNSS, INS, and LiDAR for vehicle navigation in urban environments," *IEEE Internet Things J.*, vol. 9, no. 24, pp. 24721–24735, Dec. 2022.

[5] L. Bouchard. "Combine LiDAR and cameras for 3D object detection - Waymo." Mar. 2022. [Online]. Available: https://www.louisbouchard.ai/waymo-lidar/

[6] "GM advances self-driving vehicle deployment with acquisition of LiDAR developer." Oct. 2017. [Online]. Available: https://media.gm.com/media/us/en/gm/news.detail.html

[7] J. Petit, B. Stottelaar, M. Feiri, and F. Kargl, "Remote attacks on automated vehicles sensors: Experiments on camera and LiDAR," *Black Hat Europe*, vol. 11, no. 2015, p. 995, 2015.

[8] Y. Cao et al., "Adversarial sensor attack on LiDAR-based perception in autonomous driving," in *Proc. ACM SIGSAC Conf. Comput. Commun. Security*, 2019, pp. 2267–2281.

[9] J. Sun, Y. Cao, Q. A. Chen, and Z. M. Mao, "Towards robust LiDAR-based perception in autonomous driving: General black-box adversarial sensor attack and countermeasures," in *Proc. 29th {USENIX} Security Symp. ({USENIX} Security)*, 2020, pp. 877–894.

[10] L. Fan, X. Xiong, F. Wang, N. Wang, and Z. Zhang, "RangeDet: In defense of range view for LiDAR-based 3D object detection," in *Proc. IEEE/CVF Int. Conf. Comput. Vis.*, 2021, pp. 2918–2927.

[11] J. Liu and J.-M. Park, ""Seeing is not always believing": Detecting perception error attacks against autonomous vehicles," *IEEE Trans. Dependable Secure Comput.*, vol. 18, no. 5, pp. 2209–2223, Sep./Oct. 2021.

[12] J. Tian, B. Wang, R. Guo, Z. Wang, K. Cao, and X. Wang, "Adversarial attacks and defenses for deep-learning-based unmanned aerial vehicles," *IEEE Internet Things J.*, vol. 9, no. 22, pp. 22399–22409, Nov. 2022.

[13] J. Zhang et al., "Detecting and identifying optical signal attacks on autonomous driving systems," *IEEE Internet Things J.*, vol. 8, no. 2, pp. 1140–1153, Jan. 2021.

[14] Z. Hau, S. Demetriou, L. Munoz-González, and E. C. Lupu, "Shadow-catcher: Looking into shadows to detect ghost objects in autonomous vehicle 3D sensing," in *Proc. Eur. Symp. Res. Comput. Security*, 2021, pp. 691–711.

[15] R. Matsumura, T. Sugawara, and K. Sakiyama, "A secure LiDAR with AES-based side-channel fingerprinting," in *Proc. 6th Int. Symp. Comput. Netw. Workshops (CANDARW)*, 2018, pp. 479–482.

[16] R. Meshcheryakov et al., "A probabilistic approach to estimating allowed SNR values for automotive LiDARs in "smart cities" under various external influences," *Sensors*, vol. 22, no. 2, p. 609, 2022.

[17] H. Shin, Y. Son, Y. Park, Y. Kwon, and Y. Kim, "Sampling race: Bypassing timing-based analog active sensor spoofing detection on analog-digital systems," in *Proc. 10th USENIX Workshop Offensive Technol. (WOOT)*, 2016, pp. 1–11.

[18] Y. Li, C. Wen, F. Juefei-Xu, and C. Feng, "Fooling LiDAR perception via adversarial trajectory perturbation," in *Proc. IEEE/CVF Int. Conf. Comput. Vis.*, 2021, pp. 7898–7907.

[19] E. Saeedi and Y. Kong, "Side-channel vulnerabilities of automobiles," *Trans. IoT Cloud Comput.*, vol. 2, no. 2, pp. 1–8, 2014.

[20] R. Changalvala and H. Malik, "LiDAR data integrity verification for autonomous vehicle," *IEEE Access*, vol. 7, pp. 138018–138031, 2019.

[21] N. V. Abhishek, M. N. Aman, T. J. Lim, and B. Sikdar, "DRiVe: Detecting malicious roadside units in the Internet of Vehicles with low latency data integrity," *IEEE Internet Things J.*, vol. 9, no. 5, pp. 3270–3281, Mar. 2022.

[22] K. Iehira, H. Inoue, and K. Ishida, "Spoofing attack using bus-off attacks against a specific ECU of the CAN bus," in *Proc. 15th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, 2018, pp. 1–4.

[23] C. You, Z. Hau, and S. Demetriou, "Temporal consistency checks to detect LiDAR spoofing attacks on autonomous vehicle perception," in *Proc. 1st Workshop Security Privacy Mobile AI*, 2021, pp. 13–18.

[24] K. Bahirat, U. Shah, A. A. Cardenas, and B. Prabhakaran, "ALERT: Adding a secure layer in decision support for advanced driver assistance system (ADAS)," in *Proc. 26th ACM Int. Conf. Multimedia*, 2018, pp. 1984–1992.

[25] H. Ueda, R. Kurachi, H. Takada, T. Mizutani, M. Inoue, and S. Horihata, "Security authentication system for in-vehicle network," *SEI Tech. Rev.*, vol. 81, pp. 5–9, Oct. 2015.

[26] Y. Shoukry, P. Martin, Y. Yona, S. Diggavi, and M. Srivastava, "PyCRA: Physical challenge-response authentication for active sensors under spoofing attacks," in *Proc. 22nd ACM SIGSAC Conf. Comput. Commun. Security*, 2015, pp. 1004–1015.

[27] "YDLiDAR." Accessed: Jun. 30, 2021. [Online]. Available: https://www.ydlidar.com/

[28] Y. Chen, C. Lu, and W. Chu, "A cooperative driving strategy based on velocity prediction for connected vehicles with robust path-following control," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 3822–3832, May 2020.

[29] E. E. Marvasti, A. Raftari, A. E. Marvasti, Y. P. Fallah, R. Guo, and H. Lu, "Cooperative LIDAR object detection via feature sharing in deep networks," in *Proc. IEEE 92nd Veh. Technol. Conf. (VTC-Fall)*, 2020, pp. 1–7.

[30] X. Zhang et al., "EMP: Edge-assisted multi-vehicle perception," in *Proc. 27th Annu. Int. Conf. Mobile Comput. Netw.*, 2021, pp. 545–558.

[31] D. T. Kanapram et al., "Collective awareness for abnormality detection in connected autonomous vehicles," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 3774–3789, May 2020.

[32] Y. Liu, Y. Wang, and G. Chang, "Efficient privacy-preserving dual authentication and key agreement scheme for secure V2V communications in an IoV paradigm," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 10, pp. 2740–2749, Oct. 2017.

[33] W. Whyte, A. Weimerskirch, V. Kumar, and T. Hehn, "A security credential management system for V2V communications," in *Proc. IEEE Veh. Netw. Conf.*, 2013, pp. 1–8.

[34] M. Kamal, G. Srivastava, and M. Tariq, "Blockchain-based lightweight and secured V2V communication in the Internet of Vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 3997–4004, Jul. 2021.
[35] H. Shin, D. Kim, Y. Kwon, and Y. Kim, "Illusion and dazzle: Adversarial optical channel exploits against lidars for automotive applications," in *Proc. Int. Conf. Cryptographic Hardw. Embedded Syst.*, 2017, pp. 445–467.
[36] R. A. Johnson and D. W. Wichern, *Applied Multivariate Statistical Analysis*, vol. 5. Upper Saddle River, NJ, USA: Prentice Hall, 2002.
[37] T. Sato, Y. Hayakawa, R. Suzuki, Y. Shiiki, K. Yoshioka, and Q. A. Chen, "Revisiting LiDAR spoofing attack capabilities against object detection: Improvements, measurement, and new attack," 2023, *arXiv preprint arXiv:2303.10555*.
[38] U. N. G. P. Standards and Specifications. "Lidar base specification 2023 rev A," 2023. [Online]. Available: https://www.usgs.gov/media/files/lidar-base-specification-2023-rev-a
[39] T. J. Abatzoglou, "Fast maximum likelihood joint estimation of frequency and frequency rate," *IEEE Trans. Aerosp. Electron. Syst.*, vol. AES-22, no. 6, pp. 708–715, Nov. 1986.
[40] Velodyne LiDAR. "Puck datasheet." 2019. Accessed: Nov. 10, 2023. [Online]. Available: https://velodynelidar.com/wp-content/uploads/2019/12/PuckDatasheet-Web.pdf
[41] V. V. Dixit, S. Chand, and D. J. Nair, "Autonomous vehicles: Disengagements, accidents and reaction times," *PLoS ONE*, vol. 11, no. 12, 2016, Art. no. e0168054.

Xueyang Hu received the B.S. degree in information engineering from Xi'an Jiaotong University, Xi'an, China, in 2017, and the M.S. degree in computer science and software engineering from Auburn University, Auburn, AL, USA, in 2020, where he is currently pursuing the Ph.D. degree with the Department of Computer Science and Software Engineering.

His research interests mainly focus on 5G mmWave communication and optimization in wireless networks.

Tian Liu received the B.S. degree in mathematics and applied mathematics from Sichuan University, Chengdu, China, in 2011, and the M.S. degree in probability and statistics and the Ph.D. degree in computer science and software engineering from Auburn University, Auburn, AL, USA, in 2016 and 2022, respectively.

She is a Research Staff Member with Zhejiang Laboratory, Hangzhou, China. Her research interests focus on security and privacy issues in machine learning algorithms in Internet of Things and cyber–physical systems.

Tao Shu received the B.S. and M.S. degrees in electronic engineering from the South China University of Technology, Guangzhou, China, in 1996 and 1999, respectively, the first Ph.D. degree in communication and information Systems from Tsinghua University, Beijing, China, in 2003, and the second Ph.D. degree in electrical and computer engineering from The University of Arizona, Tucson, AZ, USA, in 2010.

He is currently an Associate Professor with the Department of Computer Science and Software Engineering, Auburn University, Auburn, AL, USA. Prior to his academic position, he was a Senior Engineer with Qualcomm Atheros Inc., San Jose, CA, USA, from December 2010 to August 2011. His research aims at addressing security and performance issues in wireless networking systems, with strong emphasis on system architecture, protocol design, and performance modeling and optimization.

Diep Nguyen (Senior Member, IEEE) received the M.E. degree in electrical and computer engineering from the University of California at San Diego (UCSD), La Jolla, CA, USA, in 2008, and the Ph.D. degree in electrical and computer engineering from The University of Arizona (UA), Tucson, AZ, USA, in 2013.

He is currently a Faculty Member with the Faculty of Engineering and Information Technology, University of Technology Sydney (UTS), Sydney, NSW, Australia. Before joining UTS, he was a DECRA Research Fellow with Macquarie University, Macquarie Park, NSW, Australia, and a member of the Technical Staff with Broadcom Corporation, San Jose, CA, USA, and ARCON Corporation, Boston, MA, USA, and consulting the Federal Administration of Aviation, Washington, DC, USA, on turning detection of UAVs and aircraft, and the U.S. Air Force Research Laboratory on Anti-Jamming. His research interests include computer networking, wireless communications, and machine learning application, with emphasis on systems' performance and security/privacy.

Dr. Nguyen received several awards from LG Electronics, UCSD, UA, the U.S. National Science Foundation, and the Australian Research Council. He has served on the editorial boards for the IEEE TRANSACTIONS ON MOBILE COMPUTING, IEEE COMMUNICATIONS SURVEYS AND TUTORIALS, IEEE OPEN JOURNAL OF THE COMMUNICATIONS SOCIETY, and *Scientific Reports* (Nature).