Poster:An Adaptive High Frequency Removal Attack to Bypass Pulse Fingerprinting in New-Gen LiDARs

Yuki Hayakawa†, Takami Sato‡, Ryo Suzuki†, Kazuma Ikeda†, Ozora Sako†, Rokuto Nagata†,
Qi Alfred Chen‡, and Kentaro Yoshioka†
†Keio University; ‡University of California, Irvine

***Abstract*—LiDAR stands as a critical sensor in the realm of autonomous vehicles (AVs). Resent studies have actively researched various safety implications against LiDAR spoofing attacks. To defend against these attacks, pulse fingerprinting has been expected as one of the most promising countermeasures, and recent research demonstrates its high defense capability, especially against object removal attacks. In this poster, we report the progress in conducting further security analysis on pulse fingerprinting against LiDAR spoofing attacks. We design a novel adaptive attack strategy, the Adaptive High-Frequency Removal (A-HFR) attack, which can be effective against broader types of LiDARs than the existing HFR attacks. We evaluate the A-HFR attack on commercial LiDARs with pulse fingerprinting and find that the A-HFR attack can successfully remove over 96% of the point cloud within a 20° horizontal and a 16° vertical angle. Our finding indicates that current pulse fingerprinting techniques might not be sufficiently robust to thwart spoofing attacks. We finally discuss our future plans.**

I. Introduction

LiDAR (Light Detection And Ranging) has been integrated into autonomous vehicles (AVs) as a critical sensor.Reflecting its importance on AD systems, the security of LiDARs has been actively researched, especially for the vulnerability against LiDAR spoofing attacks [1]–[3]. However, existing LiDAR spoofing attacks still have a critical gap to be a real threat against recent AD vehicles [3]. The majority of evaluations focus only on classic LiDAR models, overlooking many recent LiDARs (new-gen LiDARs) [3]. Sato et al. [3] demonstrate that their HFR (High-Frequency Removal) attack is still effective even against the new-gen LiDARs with the timing randomization. However, the HFR attack was not effective with pulse fingerprinting that authenticates their lasers with an embedded fingerprint in the lasers.

In this poster, we report our recent progress on the further security analysis of pulse fingerprinting in new-gen LiDARs. We designed a new spoofing attack, the Adaptive HFR (A-HFR) attack, which can achieve 5 times higher frequency than the prior HFR attack even with the same laser hardware by adaptively changing the attack region. We evaluate the A-HFR attack on some commercial LiDARs with pulse fingerprinting to evaluate the generality of the attack. We finally discuss possible enhancements in fingerprint technology that could bolster defenses against such advanced spoofing techniques.

II. Background and Related Works

A. LiDAR Spoofing Attacks

The LiDAR spoofing attacks [1]–[3] have demonstrated high attack effectiveness against LiDARs. Based on the attacker's capability, there are two types of LiDAR spoofing attacks: Synchronized attacks (Sync. attack) [1] first learn the laser scanning pattern of the target LiDAR, understanding its scan timing and coverage. They prerequisite a deterministic LiDAR scanning pattern, a premise not typically valid for new-gen LiDARs. Asynchronized attacks (Async. attack) operate regardless of the victim LiDAR's scan timing. HFR attack [3] emits periodic pulses at the victim LiDAR. The attack's effectiveness varies; it is potent against some new-gen LiDARs but less so against those with pulse fingerprinting.

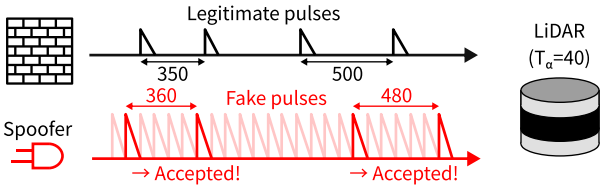


Fig. 1: Our concept to bypass pulse fingerprinting by HFR attack. The attacker could bypass the authentication by shooting fake pulses at higher frequency.

B. LiDARs with Pulse Fingerprinting

Pulse fingerprinting [4] has shown a high defense capability against LiDAR spoofing attacks while it is also originally designed for the sake of anti-interference to operate multiple LiDARs at close distances. One of the most common implementations of pulse fingerprinting (e.g. Livox Mid-360, Hesai XT32, AT128) encodes its fingerprint into the interval between two consecutive pulses. To account for nonidealities during operation, these LiDARs include a tolerance error time span T_α. The interval between pulses is randomly set between a minimum (T_{min}) and maximum (T_{max}) value.

III. Methodology

A. Attack Concept to Bypass Pulse Fingerprinting

Pulse fingerprinting is a robust defense against existing LiDAR spoofing attacks due to its signal authentication that filters out malicious pulses. However, if an attacker replicates this interval, these systems could be susceptible to spoofing.

This vulnerability is particularly pronounced in the context of HFR attacks, as illustrated in Fig. 1. Pulse fingerprinting's random pulse intervals can be exploited during an HFR attack. An effective HFR attack against pulse fingerprinting requires (1) an attack pulse interval shorter than T_α, and (2) peak power greater than that of the legitimate pulse. However, conventional

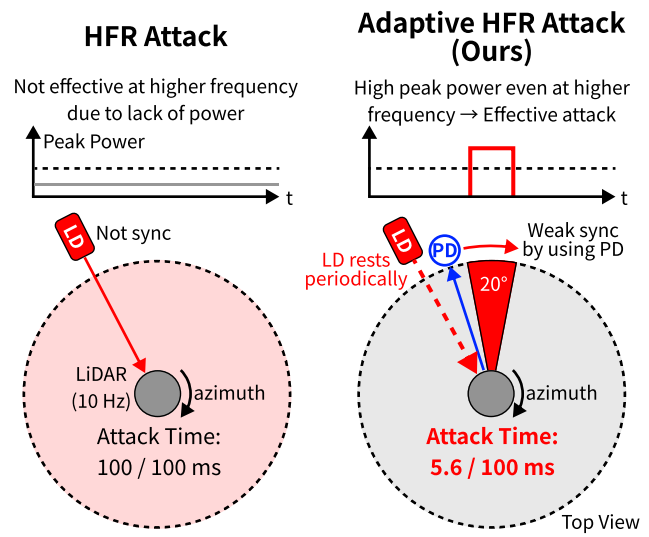


Fig. 2: Comparison of the HFR attack [3] and the A-HFR attack. A-HFR can achieve high peak power at high frequencies by reducing the attack angle through weak synchronization.

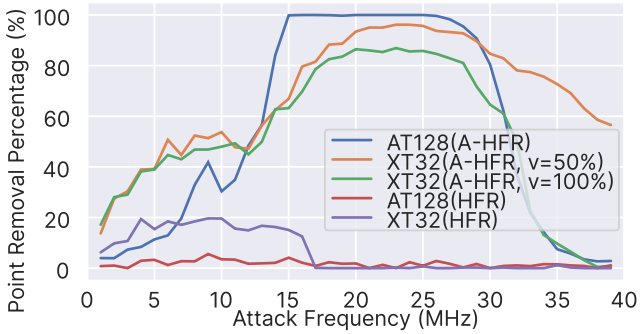


Fig. 3: Attack frequency versus point removal percentage under A-HFR attacks and conventional HFR attacks. We count points within the angle of 20° horizontally and 16° vertically.

HFR attack [3] faces a trade-off between pulse interval and peak power, making it challenging to fulfill both conditions.

B. Attack Design: Adaptive HFR Attack

As shown in Fig. 2, we developed the Adaptive HFR (A-HFR) attack, which works on the existing spoofer hardware, to overcome the trade-off between pulse frequency and power. A-HFR employs *weak synchronization* to selectively target only specific angles within the victim LiDAR's scan. This selective targeting allows the spoofer to rest and cool during non-targeted angles, averting laser driver overheating. Hence, this method enables high-frequency, high-power attacks at specific angles required to bypass the fingerprinting authentication.

IV. Evaluation

A. Evaluation Against Various Pulse Fingerprinting LiDARs

Fig. 3 displays the point removal rates for both conventional and A-HFR attacks at various frequencies, tested against AT128 and XT32 LiDARs with pulse fingerprinting. The figure demonstrates that conventional HFR attacks have a maximum success rate of only 20%, limited by thermal issues. In contrast, our A-HFR attack effectively removes over 90% of the target angle's point cloud by increasing the attack frequency.

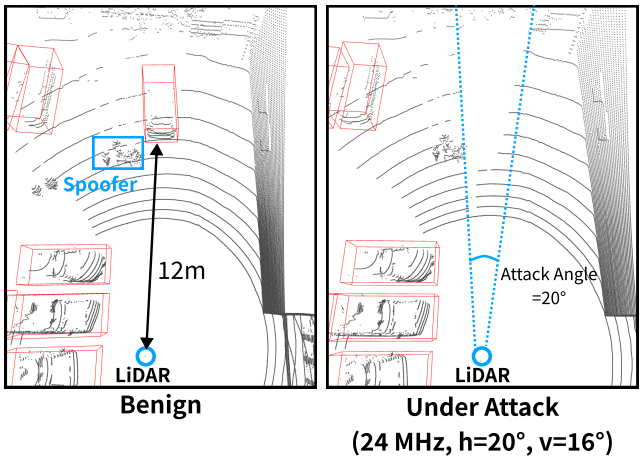


Fig. 4: A-HFR attack on Hesai XT32 to hide a real vehicle.

B. Attack Capability in the Physical World

To verify A-HFR attack effectiveness in real-world conditions, we conducted an outdoor experiment aimed at removing a car from the point cloud data of XT32. The results, shown in Fig. 4, show the complete removal of the target car point cloud. As a result, The car went undetected in the attacked data. This result shows that the A-HFR attack is a significant threat to real-world autonomous driving systems.

V. Concluding Remarks and Future Plans

In this poster, we identify a new LiDAR spoofing attack termed the A-HFR attack against LiDARs to assess the defensive efficacy of pulse fingerprinting implemented in new-gen LiDARs. We evaluate the A-HFR attack on some commercial LiDARs with pulse fingerprinting and find that the A-HFR attack is always effective against them. We plan to explore the possibility of designing more secure fingerprinting with other laser features than pulse interval.

Acknowledgements

This research was supported in part by the JST CREST JPMJCR23M4, JST PRESTO JPMJPR22PA, Amano Institute of Technology, NSF CNS-2145493, CNS-1929771, CNS-1932464, and USDOT UTC Grant 69A3552348327.

References

[1] Y. Cao, S. H. Bhupathiraju, P. Naghavi, T. Sugawara, Z. M. Mao, and S. Rampazzi, "You Can't See Me: Physical Removal Attacks on LiDAR-based Autonomous Vehicles Driving Frameworks," in *USENIX Security Symposium*, 2023.

[2] Z. Jin, J. Xiaoyu, Y. Cheng, B. Yang, C. Yan, and W. Xu, "PLA-LiDAR: Physical Laser Attacks against LiDAR-based 3D Object Detection in Autonomous Vehicle," in *2023 IEEE Symposium on Security and Privacy (SP)*. IEEE Computer Society, 2022, pp. 710–727.

[3] T. Sato, Y. Hayakawa, R. Suzuki, Y. Shiiki, K. Yoshioka, and Q. A. Chen, "LiDAR Spoofing Meets the New-Gen: Capability Improvements, Broken Assumptions, and New Attack Strategies," 2024.

[4] M. Yu, M. Shi, W. Hu, and L. Yi, "FPGA-based Dual-pulse Anti-interference Lidar System Using Digital Chaotic Pulse Position Modulation," *IEEE Photonics Technology Letters*, vol. 33, no. 15, pp. 757–760, 2021.

Poster: An Adaptive High Frequency Removal Attack to Bypass Pulse Fingerprinting in New-Gen LiDARs

Yuki Hayakawa[1], Takami Sato[2], Ryo Suzuki[1], Kazuma Ikeda[1], Ozora Sako[1], Rokuto Nagata[1], Qi Alfred Chen[2], and Kentaro Yoshioka[1]
[1]Keio University; [2]University of California, Irvine

Limitations of the prior LiDAR Spoofing Attacks

Evaluations overlook many recent new-gen LiDARs
- Prior studies [1] [2] only evaluated against 1st gen LiDARs. These attacks are not valid for new-gen LiDARs with pulse fingerprinting

Do not explore defense capability of pulse fingerprinting
- Pulse fingerprinting authenticates reflected laser pulses not to accept lasers emitted by other LiDARs

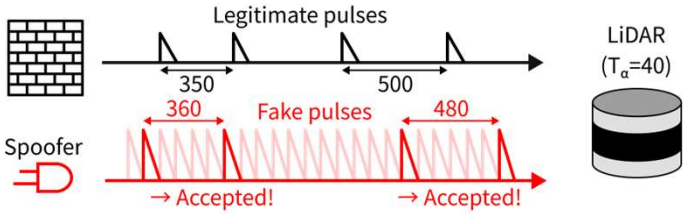
Comparison of the LiDAR spoofing attacks. ☑ indicates that the LiDAR is vulnerable to the attack.

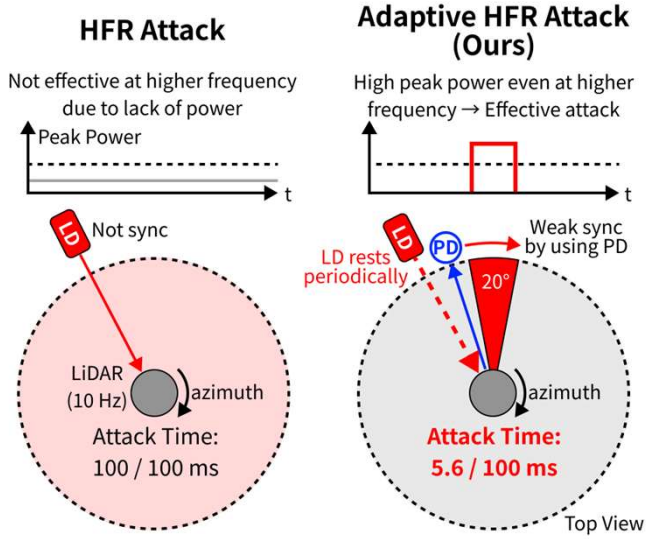
		Sync. Attack [1]	HFR Attack [2]	A-HFR Attack (Ours)
1st gen LiDAR		☑	☑	☑
New-gen LiDAR	w/ randomization	-	☑	☑
	w/ Pulse fingerprinting	-	-	☑

Adaptive HFR (A-HFR) Attack

Attack strategy and limitation of HFR
- HFR attack could effectively create a 'master key' for pulse fingerprinting by simply increasing the pulse frequency
- However, conventional HFR attack has a trade-off between pulse frequency and peak power due to overheating

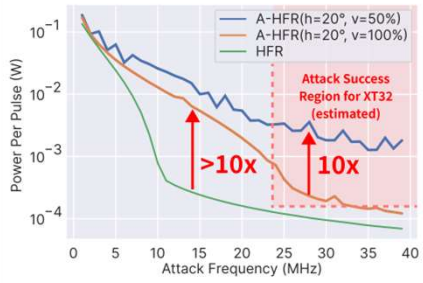
New attack design: Adaptive HFR (A-HFR) attack
- A-HFR employs **weak synchronization** to target only specific angles
- The spoofer can rest and cool during non-targeted angles, averting overheating





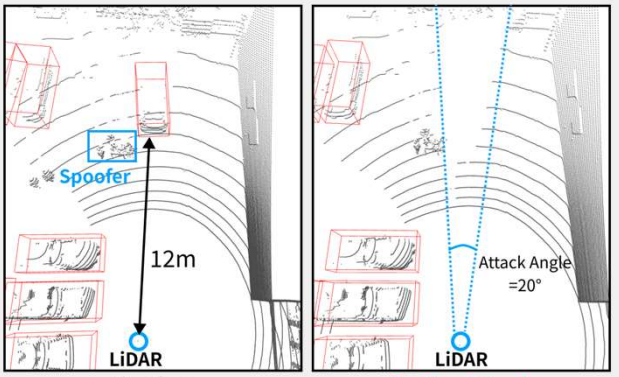
Effectiveness of Attack Angle Reduction

- **A-HFR can achieve 10x power** with horizontal reduction for 10~20 MHz
- This power boost is further enhanced by reducing vertical attack angle

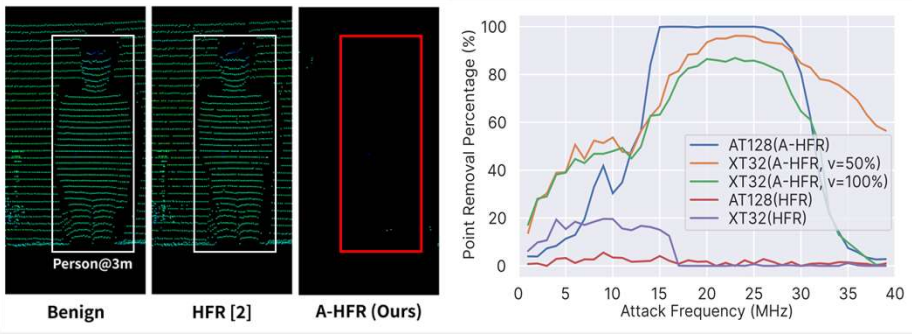


Outdoor Attack Demo

- This The vehicle becomes undetected with a **98% success rate over 15 seconds** under the attack



Indoor Attack Demo



Future Plans

- Plan to explore the possibility of designing more secure fingerprinting with other laser features than pulse interval

[1]: Yulong Cao et al., *You Can't See Me: Physical Removal Attacks on LiDAR-based Autonomous Vehicles Driving Frameworks.* In USENIX Security, 2023.
[2]: Takami Sato et al., *LiDAR Spoofing Meets the New-Gen: Capability Improvements, Broken Assumptions, and New Attack Strategies.* In NDSS 2024.