

振幅フィンガープリントを用いたセキュア LiDAR の 提案と防御性能の実証

永井 祥太^{1,a)} 速川 湧気^{1,b)} 松野 涼也^{1,c)} 野中 理沙^{1,d)} 宮城 賢美^{1,e)} 鈴木 諒^{1,f)}
池田 和真^{1,g)} 吉田 涼^{1,h)} 佐古 大空^{1,i)} 永田 禄人^{1,j)} 吉岡 健太郎^{1,k)}

概要：近年安全かつ快適な自動運転を実現するためにセンシングデバイスの一つとして LiDAR が数多く用いられている。LiDAR ではレーザを発射し反射光を取得することで対象までの距離を測定するが、攻撃者が外部からレーザを用いて距離情報を誤認させる攻撃が脅威となっている。特に、高周波のレーザを発射し攻撃を行う HFR 攻撃に対しては市販されている LiDAR のいずれも防御策を備えておらず、自動運転車にとっての大きな脅威となっている。本論文では、発射するレーザ振幅を変化させることで LiDAR に対する攻撃を防御する新しい防御手法である振幅フィンガープリント (Amplitude Fingerprinting) を提案し、シミュレーションによってこの手法の防御性能を実証する。また、振幅をナノセカンドオーダーで変調することができるレーザ基板を作成し、防御性能について考察した。

キーワード：LiDAR, 自動運転, センサセキュリティ, センサ幻惑攻撃, HFR 攻撃, 振幅フィンガープリント, 認証シグネチャ

Secure LiDAR via Amplitude Fingerprinting: Proposal and Experimental Validation of Defense Performance

SHOTA NAGAI^{1,a)} YUKI HAYAKAWA^{1,b)} RYOYA MATSUNO^{1,c)} RISA NONAKA^{1,d)} SATOMI MIYAGI^{1,e)}
RYO SUZUKI^{1,f)} KAZUMA IKEDA^{1,g)} RYO YOSHIDA^{1,h)} OZORA SAKO^{1,i)} ROKUTO NAGATA^{1,j)}
KENTARO YOSHIOKA^{1,k)}

Abstract: In recent years, LiDAR has been widely employed as one of the key sensing devices to enable safe and comfortable autonomous driving. LiDAR measures the distance to a target by emitting laser pulses and detecting the reflected light. However, adversarial attacks that use external lasers to falsify distance measurements have emerged as a serious threat. In particular, High-Frequency Replay (HFR) attacks, which involve injecting high-frequency laser signals, pose a significant danger to autonomous vehicles, as none of the commercially available LiDAR systems are equipped with effective countermeasures. In this paper, we propose a novel defense method, amplitude fingerprinting, which protects LiDAR systems by varying the amplitude of the emitted laser pulses. Through simulation experiments, we demonstrate the effectiveness of the proposed method against such attacks. Furthermore, we developed a laser driver board capable of modulating amplitude on the nanosecond scale and evaluated its defense performance.

Keywords: LiDAR, Autonomous Driving, Sensor Security, Sensor Spoofing Attack, High-Frequency Removal Attack, Amplitude Fingerprinting, Authentication Signature

¹ 慶應義塾大学
Keio, Tokyo 108-0073, Japan
a) n-shota@keio.jp
b) hykwyuk@keio.jp
c) ryoya.matsuno@keio.jp
d) gaspar@keio.jp
e) stm-m22@keio.jp
f) suzuki.ryo@keio.jp

g) kazu2080@keio.jp
h) ryo-yoshida@keio.jp
i) sako.ozora@keio.jp
j) nagatarokuto@keio.jp
k) kyoshioka47@keio.jp

1. Introduction

1.1 研究背景

近年、安全かつ快適な自動運転の実現において、LiDAR (Light Detection and Ranging) が重要な役割を果たしている。LiDAR はレーザを発射し、その反射光の飛行時間を計測することで周囲環境を高精度かつリアルタイムで三次元的に計測可能な唯一無二なセンサであるため、自動運転システムにおける主要なセンシングデバイスとして位置づけられている。

一方で、LiDAR センサに対するセキュリティ上の脅威として、外部からレーザを照射して距離計測を誤認させるセンサ幻惑攻撃が報告されている [6]。先行研究では、点群に偽の物体を注入する攻撃や [3], [5], [7]、障害物点群を消失させる攻撃 [2], [5], [10] が実証されており、特に後者は衝突事故に直結することから深刻な脅威と考えられている。さらに近年、新たな攻撃手法として High-Frequency Removal (HFR) 攻撃が注目されている [7]。HFR 攻撃は、短周期のパルス列を用いて LiDAR の計測機能を妨害する手法であり、既存の防御機構を回避する能力を有している。現在、市販 LiDAR に対する有効な防御策が存在しないことが報告されており [7]、自動運転車の安全性に対する重大な懸念となっている。

従来の LiDAR 防御技術は、主として他の LiDAR との干渉回避を目的として開発されてきた。測距タイミングのランダム化やシグネチャ付与といった既存手法は、一定の攻撃防御能力を副次的に有するものの、HFR 攻撃やその発展形である Adaptive HFR (A-HFR) 攻撃に対しては十分な防御効果を発揮できないことが明らかになっている [8]。このため、これらの新たな攻撃手法に対する効果的な対策の開発が喫緊の課題となっている。

1.2 本研究の提案

本研究では、HFR 攻撃およびその派生手法である A-HFR 攻撃に対して有効な防御策を開発することを目的とする。従来の LiDAR 防御技術は干渉回避を主眼としており、測距タイミングのランダム化やシグネチャ付与によって一定の耐性を持つものの、これら新たな攻撃手法を十分に防ぐことはできない。

そこで本研究では、LiDAR が発射するパルス対に「振幅比」を付与することで LiDAR 計測における新たなシグネチャを形成する**振幅フィンガープリント (Amplitude Fingerprinting)** を提案する。本手法は、既存の時間的・位相的なシグネチャに依存しない新しい識別軸を導入するものであり、攻撃者が模倣することが困難である点に特徴を有する。

本論文では、まず提案手法の原理を示した上で、シミュ

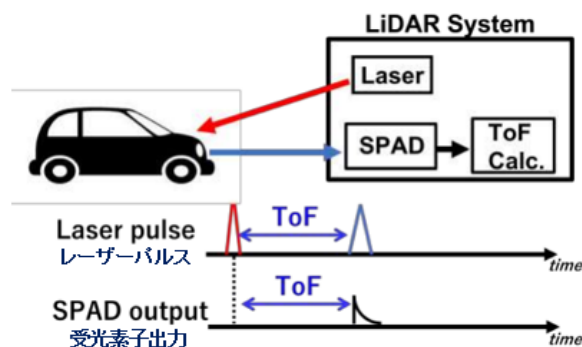


図 1: dToF LiDAR の測距原理図 [12] より引用

Fig. 1 Distance measurement principle of dToF LiDARs.

レーションにより A-HFR 攻撃に対する有効性を検証する。さらに、ナノ秒オーダーで振幅制御を可能とするレーザ基板を試作し、ハードウェア観点からの実現可能性を示すとともに、今後の課題について考察する。

2. Related Work

2.1 LiDAR の動作原理

LiDAR (Light Detection and Ranging) はレーザ光を用いて距離を計測するセンサである。代表的な測距方式として dToF (direct Time of Flight)、iToF (indirect ToF)、FMCW (Frequency Modulated Continuous Wave) の 3 種類が存在する。dToF はパルス光を射出し、その往復時間から距離を算出する方式であり、iToF は周期光の位相差を用いる。FMCW は周波数を掃引した光 (チャープ信号) を利用し、射出光と反射光の差分から距離を得るもので、元来レーダ技術に由来する。

dToF 方式は長距離測定が可能で構造も単純なため、車載 LiDAR として最も広く利用されている。本論文では自動運転車を対象とするため dToF 方式のみを扱う。dToF LiDAR は図 1 に示すように、レーザと受光素子 (PD: PhotoDiode) が同方向に配置され、射出したパルス光が物体表面で反射して戻ると PD によって受光される。レーザ射出から受光までの時間を ToF (Time of Flight) と呼び、これは光が物体まで往復する時間に相当する。したがって、対象までの距離 d は式 1 により求められる。

$$d = \frac{ToF \cdot c}{2} \quad (1)$$

2.2 HFR 攻撃

dToF LiDAR に対する主要な脅威として、センサ幻惑攻撃の存在が報告されている [6]。従来の攻撃手法には、測距タイミングに同期して点群を注入・消失させる同期攻撃や、信号を複製・再照射するリレー攻撃、受光素子を飽和させる飽和攻撃等が提案されていた [2], [5], [6], [10]。しかし、これらの攻撃は実装の複雑さや効果の限定性により、現実的な脅威としては限定的であった。

近年、新たな攻撃手法として High-Frequency Removal

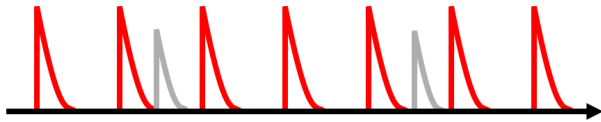


図 2: HFR 攻撃図

高周波を注入することで正規の反射光が埋もれてしまう

Fig. 2 HFR attack diagram

Injecting high frequencies buries the normal reflected light

(HFR) 攻撃が提案され、注目を集めている [7]。HFR 攻撃は、一定周期の偽パルスを照射することで LiDAR の ToF 計測を誤らせる手法である。攻撃者は対象 LiDAR の測距タイミングを事前に把握する必要がなく、単純に高頻度でパルス光を照射するだけで攻撃が成立する。(図 2)

HFR 攻撃のメカニズムは以下の通りである。攻撃パルスは受光待機時間内のランダムな位置で受光され、LiDAR が最も強いパルスを選択して距離計算を行うため、点群が本来の位置からランダムに移動し、結果として測距点の消失が発生する。さらに、受光待機時間より短い周期で攻撃を継続することで、全ての測距に対して点群消失を引き起こすことが可能である。

HFR 攻撃の最も深刻な特徴は、次世代 LiDAR に対しても有効であることが実証されている点である [7]。測距タイミングのランダム化機能を搭載した機種に対しても攻撃効果を維持しており、従来の防御技術では完全に防ぐことができない。一方、シグネチャ搭載 LiDAR では攻撃効果が大幅に制限されることが確認されているが、HFR 攻撃の攻撃強度を向上させた A-HFR 攻撃ではシグネチャ搭載 LiDAR の防御をも突破してしまうことが示されており、重大な脅威として認識されている [4], [8]。

2.3 LiDAR 防御技術

LiDAR における防御技術の多くは、もともと外部環境に起因する「干渉問題」への対策として導入されたものである。しかし、これらの技術の中にはセンサ幻惑攻撃の防御としても機能するものが存在することが近年明らかになっている。すなわち、干渉回避を目的として発展してきたランダム化やシグネチャ付与は、攻撃者が生成する偽パルス光を識別あるいは無効化できるため、結果的に攻撃対策としても有効に作用する。本節では、こうした防御手法の背景と進化を整理し、代表的な機能として干渉回避機能およびシグネチャ搭載について述べる。

2.3.1 干渉問題の背景

自動運転システムにおける LiDAR の普及に伴い、同一空間に複数の LiDAR が存在する状況が一般的となりつつある。従来の第一世代 LiDAR (例: VLP-16[1], VLP-32c[11])

はシンプルな測距システムの組み合わせにより三次元点群を取得する方式を採用していたが、同一波長帯の赤外光を利用するため、外部の LiDAR から発せられた測距光を受信してしまう干渉問題が発生していた。この干渉は測距精度の低下を招くとともに、自動運転における安全性にも影響を与えるため、早期から解決が求められていた。

第一世代 LiDAR では、同一車両内の複数センサ間で測距方向を協調的に制御し干渉を回避する「位相固定機能」が搭載されていた。しかしこの方式は自身の制御下にある LiDAR に限られ、他車両に搭載された LiDAR との干渉に対しては無効であった。この制約を克服するため、次世代 LiDAR ではより高度な干渉回避機能が導入されている。

2.3.2 次世代 LiDAR における干渉回避機能

次世代 LiDAR は受光素子や読み出し回路を単一チップに集積化することで、低コストかつ高い拡張性を実現すると同時に、チップ上での高度な信号処理を可能とした。この技術的進展により、外部からの干渉に対処する複数の機能が搭載されている。代表的なものとして図 3 のように以下の 2 点が挙げられる。

(1) 測距間隔のランダム化

測距開始タイミングをランダムに変動させることで、他 LiDAR とのタイミング一致による広範囲の測距エラーを軽減する手法である [10]。この方式により測距の安定性は向上し、さらに副次的効果として外部からの同期攻撃の無効化が可能となる。しかしながら、測距時間の推定を必要としない HFR 攻撃 [7] に対しては依然として脆弱であり、センサ幻惑攻撃に対する包括的防御策とはなりえない。

(2) シグネチャ技術

測距信号へのシグネチャ付与により、射出時に付与した認証情報を受光信号から抽出・照合し、自身の反射光と外部由来信号を区別する方式である。HFR 攻撃に対して特に有効とされる代表的手法が、パルス間隔認証である。

2.3.3 パルス間隔認証

パルス間隔認証は、2つのパルス光間の時間的間隔をアナログ認証情報として活用する手法である [9], [13]。従来の単一パルス光による測距とは異なり、時間差を付加した2つのパルス光を同一方向に連続照射する。本手法の核心となる原理は、「同一物体により反射された2つのパルス光間の時間差は、外部要因の影響が無視できる場合において、反射前の時間差と等しく保持される」という物理的特性に基づくものである。たとえ対象物が移動していた場合であっても、パルス間隔がナノ秒オーダーで十分に短ければ、ドップラー効果等による時間差の変化は極めて小さく、実質的に無視できる。したがって、受信された2つのパルス光の時間差が照射時の設定と一致するかどうかを検証することで、パルス対が正規のものであるかを判定可能となる。時間差が一致しない、あるいは明確なペアとして認識されない受信信号は、外部からの不正な干渉または攻撃に

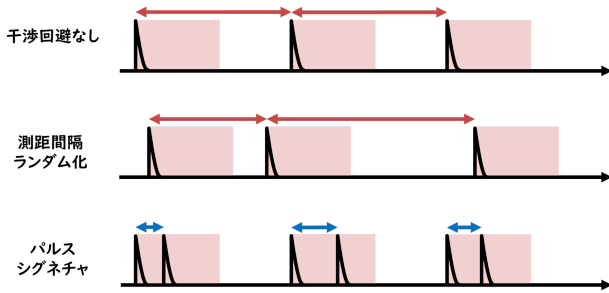


図 3: 干渉対策手法の比較

Fig. 3 Comparison of interference countermeasure methods

よるものであると見なされ、無視される。

しかしながら、パルス間隔認証にも限界が存在することが明らかになっている。近年提案された Adaptive HFR (A-HFR) 攻撃 [4], [8] では、攻撃者が高周波レーザパルスを放射し、あらゆる時間間隔を網羅することで、パルス間隔のシグネチャ認証を突破する手法が実証されている。このため、時間的シグネチャのみに依存する既存の防御技術では、進歩した攻撃手法に対して十分な防御効果を提供できないことが課題となっている。

3. 提案手法

3.1 提案の背景と狙い

既存の防御手法は、その多くが当初 LiDAR 同士の干渉問題を解決することを目的として導入されたものである。測距タイミングのランダム化やシグネチャ付与といった技術は、後にセンサ幻惑攻撃に対しても一定の防御効果を持つことが確認されている。しかし、非同期に偽パルスを照射する HFR 攻撃や A-HFR 攻撃に対しては、これらの手法のみでは依然として十分な防御性能を確保できないことが報告されている [4], [7], [8]。特に A-HFR 攻撃では図 4 のようにパルス間隔認証を突破できることが検証されており、[4], [8] 早急な対策が求められている。

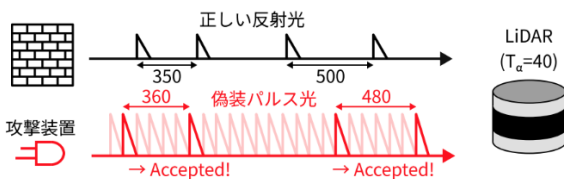


図 4: HFR によるパルス間隔認証の突破

Fig. 4 Breaking through authentication using pulse interval authentication with HFR

本研究では、この課題を克服するために振幅フィンガープリントを提案する。HFR 攻撃の本質的な制約として、高周波で連続的にパルスを照射する際に振幅変調を行うことは技術的に極めて困難である点が挙げられる。従来のパルス間隔認証が「時間差」のみをシグネチャとして利用していたのに対し、本手法では「パルス対の時間間隔」と「振

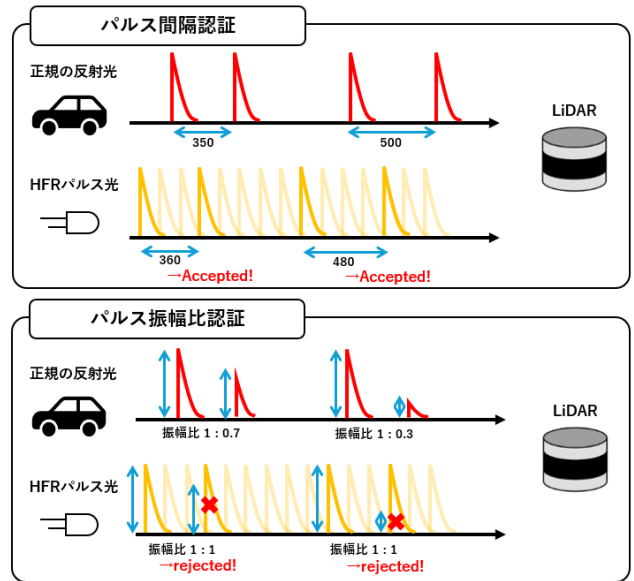


図 5: パルス間隔認証と振幅フィンガープリントの認証過程の比較

Fig. 5 Comparison chart of pulse interval authentication and amplitude fingerprint authentication processes

幅比」という二つの物理量を組み合わせてシグネチャを構成する。これにより、攻撃者は正規パルスの時間間隔だけでなく振幅比まで同時に模倣する必要が生じる。しかし、HFR 攻撃は通常一定振幅のパルス列を用いるため、多様な振幅比への対応は困難である。仮に振幅変調が可能であったとしても、時間と振幅の 2 次元における組み合わせ数が膨大となるため、攻撃成功確率は著しく低下する。

3.2 振幅フィンガープリントの基本原理

本研究で提案する振幅フィンガープリントは、従来のパルス間隔認証における「時間間隔」のみに依存する方式を拡張し、パルス対の振幅比を追加的に利用することでシグネチャを構成する。図 5 に認証過程の概要を示す。

シグネチャ生成過程: LiDAR は 1 回の測距処理において、時間差 Δt と振幅比 $r = A_2/A_1$ を持つ 2 つのパルスを同一方向に射出する。ここで、 A_1 、 A_2 はそれぞれ第 1 パルス、第 2 パルスの振幅である。これらの値は測距ごとにランダムに設定され、内部に記録される。

認証判定過程: 受光されたパルス対から時間間隔 $\Delta t'$ と振幅比 r' を抽出し、射出時に設定したシグネチャ $(\Delta t, r)$ との一致を確認する。認証成功の条件は以下の通りである：

$$|\Delta t' - \Delta t| < \epsilon_t \quad \text{かつ} \quad |r' - r| < \epsilon_r$$

ここで、 ϵ_t 、 ϵ_r はそれぞれ時間間隔と振幅比の許容誤差である。

HFR 攻撃に対する優位性: 従来の HFR 攻撃は、図 4 に示すように一定振幅 A_{attack} のパルス列を照射する。この場合、攻撃パルス対の振幅比は常に $r_{\text{attack}} = 1$ となり、

正規パルスの振幅比 $r \neq 1$ と一致しないため、認証に失敗する。

3.3 設計要件と課題

提案手法を実装するためには、以下の要素技術が必要となる。

1. 高速振幅変調回路: 現在の商用 LiDAR に搭載されているレーザ駆動回路は、発射パルスのタイミング制御には対応しているものの、振幅をナノ秒オーダーで変調する機構は有していない。したがって、安価かつ小型で高速に振幅を制御できる回路の設計が不可欠である。

2. 受光後のシグネチャマッチング回路: 振幅フィンガープリントを実現する上で鍵となるのが、受光後に時間間隔と振幅比を同時に照合するシグネチャマッチング回路である。この回路は、受光素子から出力されたパルス対を単なる有無検出に留めず、各パルスの強度を高精度に取得し、送信時に設定されたシグネチャ（間隔+振幅比）と比較する役割を担う。正規パルス対に固有の「時間間隔+振幅比」の特徴を確実に保持したまま復元し、攻撃者が生成した偽パルスとの識別精度を高いレベルで確保することが可能となる。

4. シミュレーションによる評価

本章では、提案する 振幅フィンガープリント による攻撃耐性を評価するため、LiDAR 測距の挙動を模擬可能なシミュレータを用いた検証を行った。シミュレータは LiDAR のパルス送受信処理を点単位で再現し、外部からのスプーフィング信号や環境雑音を重畳可能である。

4.1 評価環境の構築

評価には、高精度 LiDAR センサをシミュレータで模擬したものを開発し、利用した。センサは 192 水平方向 × 56 垂直方向の走査を行い、各走査点ごとに受信窓を設定し、環境反射信号、太陽光雑音、およびスプーフィング信号を重畳して処理する。外乱モデルには DummyOutdoor を用い、対象物体は反射率 0.8 の壁（距離 50 m）として設定した。スプーフィング信号は DummySpoofContinuousPulse により生成し、パルス周波数やパルス幅を任意に設定して LiDAR の受信窓に挿入した。評価は以下の 4 条件で実施した。

1. 認証なし（基準）
2. パルス間隔認証（2 パルス構成）
3. パルス間隔認証（3 パルス構成）
4. パルス間隔認証 + 振幅比認証（2 パルス構成）

4.2 評価項目

評価指標として以下を用いた。

点群消失率: LiDAR が生成すべき点群のうち、攻撃によ

り失われた点の割合。これによりスプーフィング攻撃が LiDAR の認識に及ぼす影響を定量化する。

可視化による直観的評価: 壁面を対象とした点群画像を描画し、認証方式の有無による差を確認する。特に、提案手法である振幅フィンガープリントの有効性を「パルス間隔認証のみ」と比較することで、耐攻撃性の向上を確認する。

4.3 結果

図 7 に可視化結果を示す。攻撃なしの場合（左）、壁面は正しく認識される。一方でパルス間隔認証のみを導入した場合（中央）、スプーフィング信号が優勢となり、壁面が完全に消失した。これに対し、振幅比を併用した認証（右）では、壁面が再び視認可能となり、攻撃信号に対する耐性が大幅に向上することが確認された。

図 6 に点群消失率の変化を示す。認証なしの場合、攻撃周波数が数 MHz に達すると点群はほぼ完全に消失する。パルス間隔認証のみを導入した場合も、周波数の上昇に伴い消失率は急増し、高周波領域では 90% 以上の点が消失した。これに対し、振幅比を組み合わせた場合は消失率が大幅に抑制され、15 MHz においても約 20% 程度に留まった。以上より、提案手法である振幅フィンガープリントを併用することで、従来のパルス間隔認証に比べ、スプーフィング攻撃下での LiDAR 点群の保持率が大幅に改善されることを確認した。

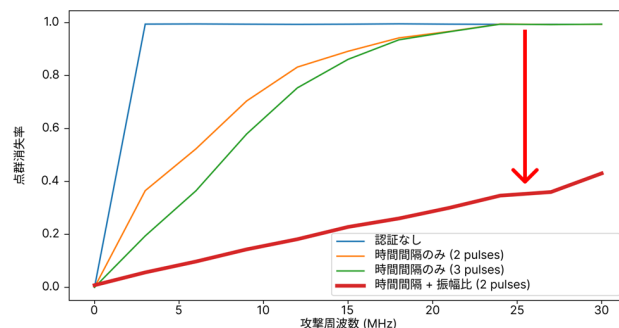


図 6: シミュレーションによる点群消失率の結果

Fig. 6 Results of point cloud loss rate based on simulation

5. レーザモジュールの実装

5.1 ハードウェア設計

本研究で提案する振幅フィンガープリントを実機で検証するため、振幅変調が可能なパルスレーザ駆動回路を設計・実装した。設計方針として、レーザダイオードに供給される電流パルスの振幅を制御可能とすることを目標とし、そのためにエネルギー蓄積素子であるキャパシタに充電される電荷量を制御する方式を採用した。

具体的には、キャパシタへの充電時間を変化させることで供給電流を変調し、結果としてレーザの出力振幅を制御

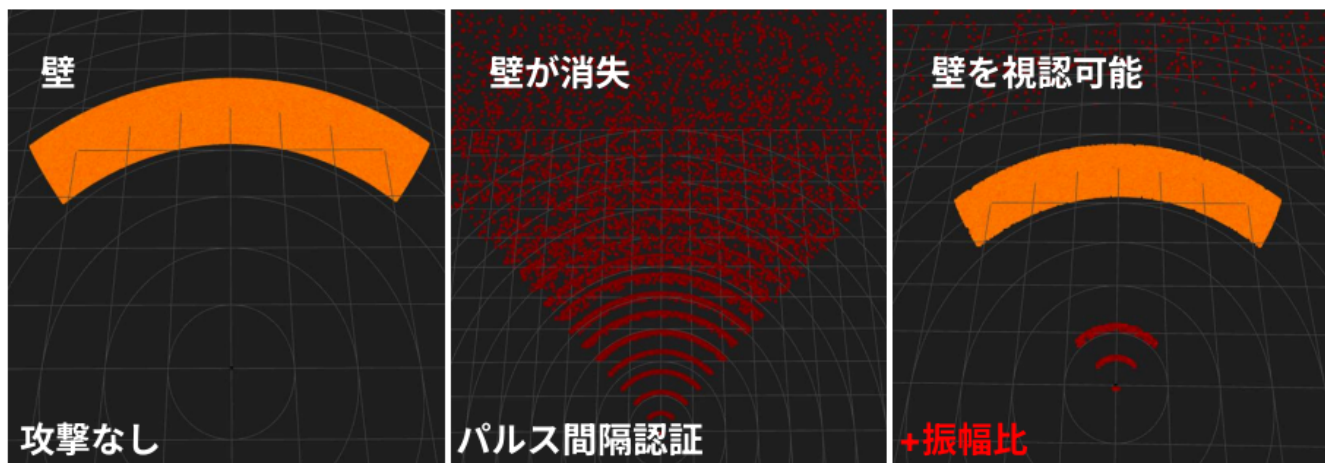


図 7: シミュレーションによる攻撃時点群比較
Fig. 7 Comparison of attack points using simulation

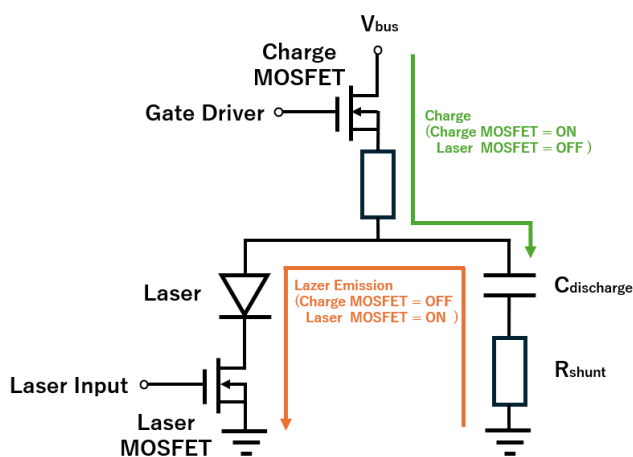


図 8: レーザ振幅変調回路
Fig. 8 Laser amplitude modulation circuit diagram

できるようにした (図 9)。高速応答を実現するため、キャパシタの充放電制御には GaN FET を用いたスイッチング回路を構成した。この結果、キャパシタ充電時間の制御における遅延を最大で数十ナノ秒オーダーに抑えることに成功し、振幅シグネチャの実現に必要な高速変調が可能であることを示した。

図 8 に本研究で実装した回路図を示す。回路の中心には LTC4446 を用いたゲートドライバを配置し、EPC2204 GaN FET をスイッチ素子として用いている。レーザ発射制御用の GaNFET の他にキャパシタ充電時間制御用の GaNFET を追加することによって、キャパシタへの充電時間を制御しキャパシタに貯まる電荷量を操作しレーザ振幅を自由に制御することが可能となった。

本回路設計により、レーザの発光タイミングと振幅の両方をナノ秒スケールで制御することが可能となり、シミュレーションで示した振幅フィンガープリント方式の実装基盤を提供する。次節では、本モジュールを用いた実験環境および動作検証について述べる。

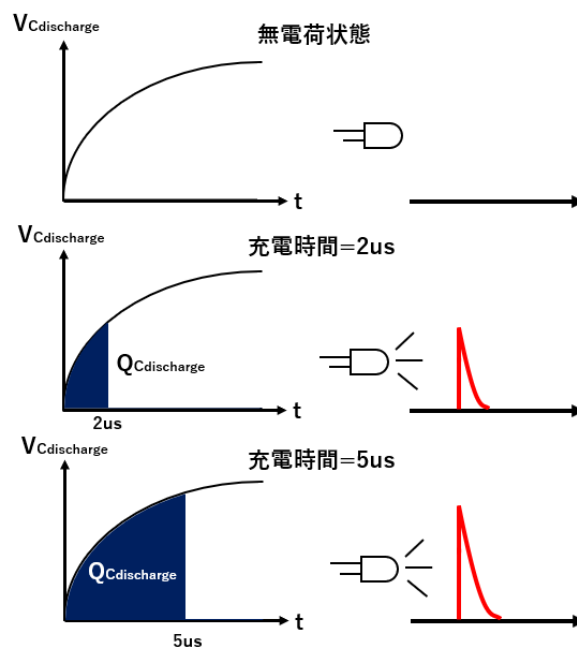


図 9: キャパシタへの充電時間を変調することによりレーザ振幅を変調可能となる

Fig. 9 Modulation of the laser pulse amplitude is achieved by varying the capacitor charging time.

5.2 レーザ振幅変調回路の動作検証

本節では、設計・実装したレーザ振幅変調回路の基本的な動作特性を検証する。検証環境としては、実装基板をオシロスコープに接続し、レーザ発射に用いるキャパシタの電圧波形を直接観測した。

図 10 に示す通り、キャパシタの充電時間を制御することにより、レーザ発射用キャパシタの電圧が変化の様子が確認された。すなわち、本回路によりナノ秒オーダーでの振幅変調に必要な電圧制御が可能であることが示された。

さらに、充電時間とキャパシタ電圧の関係を定量的に評価した結果を図 11 に示す。本回路では、抵抗値 $R = 975, \Omega$ 、



図 10: レーザキャパシタ電圧の観測結果

Fig. 10 Measured waveform of capacitor voltage for laser emission

キャパシタ合計容量 $C = 2.8, \text{nF}$ を用いており、理論的な時定数は $\tau = RC = 2.73, \mu\text{s}$ と見積もられる。図 11 の実測結果は指数関数的な充電曲線に概ね一致するが、理論値との間に一定の差異が確認された。この誤差の要因としては、基板配線による寄生成分（インダクタンス）、実装部品のばらつき、ならびに測定系における寄生抵抗・容量の影響が考えられる。

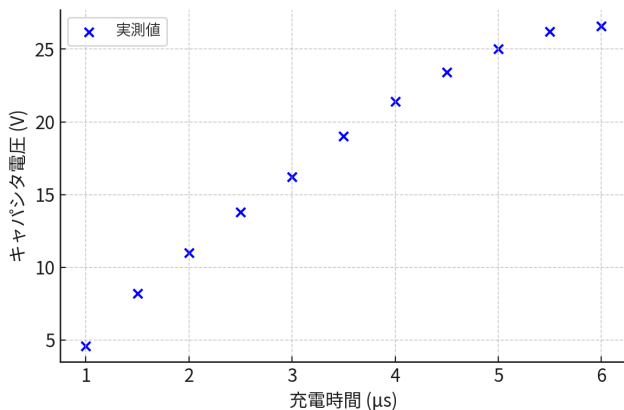


図 11: キャパシタ電圧と充電時間の関係 ($V_{\text{bus}} = 30 \text{ V}$)

Fig. 11 Relationship between capacitor voltage and charging time ($V_{\text{bus}} = 30 \text{ V}$)

以上の結果より、本回路は理論的挙動と整合的に動作することが確認され、振幅比を認証シグネチャとして利用するための基盤技術として有効に機能することが示された。

一方で、観測結果からは振幅の変動に数%程度の揺らぎが存在することも明らかになった。これはキャパシタ充電回路における配線インピーダンス等の影響によるものと推測される。したがって今後は、受光系におけるシグネチャ判定回路がこの程度の揺らぎを許容できるよう設計する必要がある。以上の結果より、提案手法に必要なナノ秒オーダーでの振幅制御が実現可能であることが確認された。

6. 考察と課題

本研究では、HFR 攻撃や A-HFR 攻撃といった従来防御手法では十分に対処できなかったセンサ幻惑攻撃に対し、新たな認証方式として振幅フィンガープリントを提案し、その有効性をシミュレーションおよびハードウェア試作によって検証した。その結果、従来のパルス間隔認証を単独で用いる場合に比べ、点群消失率を大幅に低減できることを示した。

一方で、提案手法を実際の車載 LiDAR システムへ適用するためには、いくつかの技術的課題が残されている。第一に、受光系でのリアルタイム認証処理の実現である。振幅情報を高精度に判定するためには、従来の受光回路では性能が不十分であり、ナノ秒オーダーでの信号強度検出が可能とする高速・高分解能な回路設計が不可欠である。第二に、長距離測距における信頼性が課題となる。本手法ではパルスの一方を意図的に減衰させるため、距離が増すにつれて弱いパルスの検出が困難となり、結果的に認証精度や測距性能が低下する可能性がある。この問題に対処するには、微小な振幅差でも判定可能な受光系の導入や、シグネチャ設計における振幅比の最適化が必要である。

以上より、提案手法は有効性が確認された一方で、受光回路の高度化やシステム設計上の工夫が今後の課題として残されている。

7. 結論

本研究では、HFR 攻撃および A-HFR 攻撃に対して有効な新たな防御手法として振幅フィンガープリントを提案した。本手法は、従来のパルス間隔認証に加えて「振幅比」をシグネチャとして利用することで、攻撃者による模倣を困難にし、耐攻撃性を飛躍的に向上させる点に新規性を有する。

シミュレーション評価により、従来方式では 90% 以上の点群が消失する条件下においても、提案手法を適用することで消失率を 20% 程度に抑制できることを確認した。また、実機回路の試作実験により、ナノ秒オーダーでの振幅制御が実現可能であることを示し、提案手法の実装基盤を提供した。

本研究の成果は、従来の防御方式では防ぎきれなかった HFR 系攻撃に対する有効な対策を提示し、自動運転における LiDAR セキュリティの新たな方向性を示すものである。今後は、受光系回路の改良やシグネチャ設計の最適化を通じて、商用 LiDAR への適用可能性をさらに高めることが期待される。

参考文献

- [1] Vlp-16 user manual. <https://velodynelidar.com/wp-content/uploads/2019/12/63-9243-Rev-E-VLP-16-User->

Manual.pdf. (Accessed on 01/07/2023).

- [2] 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.
- [3] Y. Cao, C. Xiao, B. Cyr, Y. Zhou, W. Park, S. Rampazzi, Q. A. Chen, K. Fu, and Z. M. Mao. Adversarial sensor attack on lidar-based perception in autonomous driving. In *2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19)*, pages 2267–2281, 2019.
- [4] Yuki Hayakawa, Takami Sato, Ryo Suzuki, Kazuma Ikeda, Ozora Sako, Rokuto Nagata, Ryo Yoshida, Qi Alfred Chen, and Kentaro Yoshioka. Breaking the shield: Systematic security analysis on pulse fingerprinting lidar systems for autonomous driving. *IEEE Sensors Journal*, 2025.
- [5] 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)*, pages 710–727. IEEE Computer Society, 2022.
- [6] J. Petit, B. Stottelaar, M. Feiri, and F. Kargl. Remote attacks on automated vehicles sensors: Experiments on camera and lidar. In *Black Hat Europe*, volume 11, page 2015, 2015.
- [7] Takami Sato, Yuki Hayakawa, Ryo Suzuki, Yohsuke Shiiki, Kentaro Yoshioka, and Qi Alfred Chen. Lidar spoofing meets the new-gen: Capability improvements, broken assumptions, and new attack strategies. *arXiv preprint arXiv:2303.10555*, 2023.
- [8] Takami Sato, Ryo Suzuki, Yuki Hayakawa, Kazuma Ikeda, Ozora Sako, Rokuto Nagata, Ryo Yoshida, Qi Alfred Chen, and Kentaro Yoshioka. On the realism of lidar spoofing attacks against autonomous driving vehicle at high speed and long distance. In *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, 2025.
- [9] H. Seo, H. Yoon, D. Kim, J. Kim, S.-J. Kim, J.-H. Chun, and J. Choi. Direct tof scanning lidar sensor with two-step multievent histogramming tdc and embedded interference filter. *IEEE Journal of Solid-State Circuits*, 56(4):1022–1035, 2021.
- [10] H. Shin, D. Kim, Y. Kwon, and Y. Kim. Illusion and dazzle: Adversarial optical channel exploits against lidars for automotive applications. In *International Conference on Cryptographic Hardware and Embedded Systems*, pages 445–467. Springer, 2017.
- [11] Velodyne Lidar. Ultra puck surround view lidar sensor. <https://velodynelidar.com/products/ultra-puck/>. Accessed: 2025-08-10.
- [12] K. Yoshioka. A tutorial and review of automobile direct tof lidar socs: Evolution of next-generation lidars. *IEICE Transactions on Electronics*, advpub:2021CTI0002, 2022.
- [13] 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*, 33(15):757–760, 2021.