SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

LiDAR ベース物体認識システムの攻撃耐性評価用シミュレータ
A Simulator for Evaluating Attack Resistance of LiDAR-based Object Recognition Systems

一ノ瀬竜矢† 上田 晋生† 深津 勇貴† 久保 中† 吉田 直樹† 松本 勉†
Ryuuya Ichinose Shinsei Ueda Yuki Fukatsu Ataru Kubo Naoki Yoshida Tsutomu Matsumoto

キーワード ハードウェアセキュリティ，LiDAR，自動運転，シミュレータ

あらまし

自動車の安全な走行を補助する先進運転支援システム（ADAS）は，自動緊急ブレーキ搭載義務化の例にみられるように一般に広く普及している．また，ドライバーによる操縦が一切不要な完全自動運転の実用化に向けて様々な技術開発が自動車業界を中心に進められている．ADAS を搭載した自動車や自動運転車は，ステレオカメラやレーダー，LiDAR（Light Detection and Ranging），超音波センサなどのセンサで計測したデータを元に周囲の走行環境を認識し，緊急ブレーキ機能や車線維持機能などといった運転支援機能を実現する．特に，自動運転車に用いられる測距センサの中でも赤外レーザーを利用して測距を行う LiDAR は数㎜単位の高精度な測距が可能で，障害物までの距離だけでなく障害物の形状推定にも向く性質を活かして安全な走行に役立てるシステムが盛んに開発されている．

一方で，LiDAR に異常な点群データを出力させる攻撃の脅威が指摘されている．光パルス伝播方式の LiDAR への反射光偽装攻撃として，実際の距離とは異なる距離を出力させる攻撃が提案されている[1][2].

これらの攻撃は LiDAR の出力データを利用する後段のアルゴリズムの動作を妨げる可能性がある．例えば LiDAR の出力点群を基に周辺の歩行者や車両の位置を検出するシステムの場合，LiDAR への攻撃によって自動車が周囲の状況を正確に把握できず衝突事故につながるおそれがある．そのため，ADAS 搭載車や自動運転車の安全性を保証するためにはセンサへの攻撃が車両の運転制御に与える脅威を検証し，事前に対策を施すことが重要である．

本研究では，LiDAR への攻撃が点群データを入力とする物体認識システムの認識結果に与える影響を，シミュレータを用いて評価する．

シミュレータは数値解析ソフトウェア MATLAB とゲームエンジン UnrealEngine4 を用いて実装した．シミュレータは自動車をモデル化したセンサ部・制御部・駆動部に加え，走行する空間をモデル化した環境部によって構成され，走行中の自動車のセンサに対する様々な物理的な攻撃が引き起こす最終的な運転制御への影響をシミュレートすることができる．このシミュレータを用いて LiDAR への攻撃によって発生する異常な出力点群を作成し，提案されている様々な物体認識アルゴリズムに入力したときの認識精度への影響を評価する．

本研究の一部は，国立研究開発法人新エネルギー・産業技術総合開発機構（NEDO）の委託業務「AI エッジデバイスの横断的なセキュリティ評価に必要な基盤技術の研究開発」によって実施されたものである．

参考文献

[1] Hocheol Shin, et al. “Illusion and Dazzle: Adversarial Optical Channel Exploits Against Lidars for Automotive Applications” International Conference on Cryptographic Hardware and Embedded Systems (CHES),2017.

[2] 相馬一樹，藤本大介，松本 勉，”反射光なりすまし攻撃に対する測距 LIDAR の計測セキュリティ，” 電子情報通信学会 暗号と情報セキュリティシンポジウム SCIS 2017, 2E1-2, 2017 年 1 月.

† 横浜国立大学，〒240-8501 横浜市保土ケ谷区常盤台 79-7
Yokohama National University, 79-7 Tokiwadai, Hodogaya-ku, Yokohama 240-8501, Japan