

PointPillars を用いた LiDAR ベース物体検出に対する物理的偽装攻撃の影響評価

M2022SC009 中岡透輝

指導教員: 河野浩之

1 はじめに

自動運転車は、カメラやレーダー等の車載センサで取得したデータを元に周囲の環境を認識、判別して緊急ブレーキや車線維持などの機能を実現している。中でも LiDAR センサはレーザー光を照射することで点群データを取得し、対象物との距離や形状を認識し物体検出を行う。そして、識別結果から車両や歩行者などを区別し安全な自動走行を可能にしている。

LiDAR は他の車載センサであるミリ波レーダーやカメラと比べ高い精度やロバスト性がある。また、表 1 によると、LiDAR の市場規模は 2030 年では 2022 年の約 15 倍となる 86 億 1,100 万ドルであるとされており、自動運転の要となるセンサと言われている。一方で、そのような LiDAR の物体認識に対し、反射光を偽装し異常な点群データを出力させる攻撃 [1] や、敵対的物体を生成し誤検出を誘発する攻撃手法 [2] が発見されている。これにより、車両や歩行者が自車の周囲に出現した場合であっても、それが正しく認識されず、ブレーキ等の車の制御を行うシステムに影響が生じ、衝突などの事故が発生することが考えられる。しかし、これらの攻撃は攻撃側の機器製作のコストや前提知識の面で必ずしも実現可能性が低いとは言えない。そこで、先行研究では新たな物理的偽装攻撃 [3] を定義している。

本研究では、物理的偽装攻撃を想定し、車両側面の LiDAR 点群を欠損させることによる車両検出への影響について評価を行う。LiDAR ベースの物体検出モデルである PointPillars を用いて、複数パターンの欠損を施した車両側面の点群データを物体検出モデルへの入力とする。そして、車両検出に影響を及ぼす最小に近い点群欠損範囲を算出し、攻撃の実現性について検討する。

表 1: LiDAR の市場規模 [4]

年	市場規模
2022 年	5 億 5,500 万ドル
2030 年	86 億 1,100 万ドル

2 LiDAR への物理的偽装攻撃とその検証

2.1 LiDAR への攻撃とその方法

LiDAR への攻撃手法を図 1 に示す。LiDAR への攻撃は、あるパターンのレーザー光線を LiDAR の受光部に特定のタイミングで照射して行う。これにより、点群情報が形成されシステムが誤認識を引き起こすことを可能にするという仕組みである。具体的にはこの方法によって、取得した点群データの除去や追加、偽造物体の注入が可能になり、結果として存在しない物体をあたかも存在し

ているように見せかけたり、あるいは、目の前の物体の存在を消すことなどを可能にする。

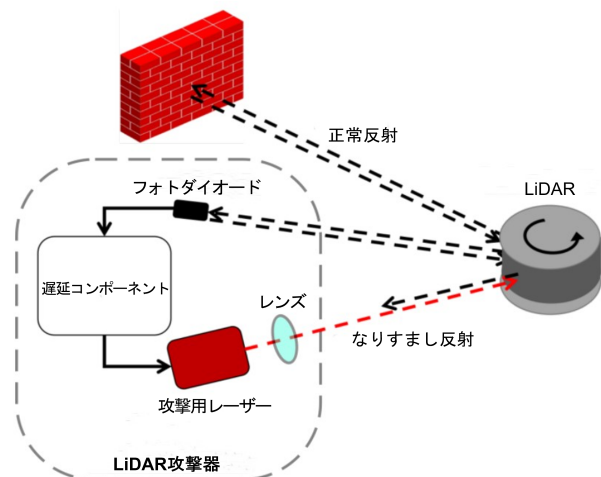


図 1: LiDAR への攻撃手法 [1]

2.2 物理的偽装攻撃の検証に関する先行研究

Cao らは [1]、反射光なりすまし攻撃によって点群 60 点までを偽装できるという仮定のもと敵対的サンプルを被害者車両の前方 7m に生成した。実験の結果、実際には存在しない障害物を物体認識システムに誤認識させる攻撃を確認した。そして、偽装された点群は全て車両であると誤認識され、実際の車両の点群よりも少ない点群で車両を偽装できることを明らかにした。

Tu らは [2]、敵対的物体を設計し車両の屋上に設置することで、車両検出不可を可能にしている。これまでの研究では、レーザー光線を直接 LiDAR に照射することで可能にしていたが、レーザーの固定角周波数、光の投影形状などの問題で、必ずしも物理的に実現可能とは限らないということを Tu らは指摘した。そこで、物理的に実現可能な LiDAR に対する普遍的な敵対攻撃として、敵対的物体を設置するという提案を行った。機械学習モデルを用いて車両の特徴を考慮した形状生成を行い、敵対的物体を生成した。それをモデル下で車両の屋上に設置した。実験の結果、設置時と非設置時とを比較して検出率が約 30%まで低下した。また、3 つの物体検出モデル (PIXOR, PointRCNN, PointPillars) のそれぞれにおいて検出率低下を達成した。

深津らは [3]、対象物体に対して細工を施すことで、LiDAR ベース物体検出を欺くような物理的偽装攻撃を新たに定義し、LiDAR の点群欠損による車両検出への影響評価を行った。Tu らと異なる点は、新たに物体を生成するのではなく、車両の既存点群を欠損させる攻撃を想定し

たことである。尚、点群を欠損させる現実的な手段として赤外線カットフィルムを示しており、実機でもその効果を証明している。赤外線カットフィルムとは、赤外線の波長である 780nm～1nm の波長の電磁波をカットすることができ、LiDAR の波長である 900nm 前後をカットすることで点群を欠損させることができるというものである。これにより、従来の攻撃方法と比べより容易に車両に対する攻撃を可能にした。

3 物理的偽装攻撃に対する評価領域の拡張

3.1 先行研究の実験内容

深津らは、複数のパターン欠損を伴う車両の点群の位置を調べ、有効な点群除去位置の探索を行った。

自車両から 7m 離れた車両ひとつを対象とし、上下 2 分割し片方の点群をそれぞれ欠損させた場合は、下半分を欠損させた場合のみ車両検出不可となった。続けて、車両背面下部をさらに縦に 3 分割し点群欠損を行った結果、中央位置の除去のみが検出不可となり、横幅 0.4m が車両検出を不可能にさせることができる限界の長さに近いことを確認した。このことから、横方向では中央の位置が重要であることが確認された。

結果として、車両検出に影響を及ぼす最小に近い点群欠損面積として、車両背面全体の面積の約 15 % の点群を欠損できればよいことを明らかにした。

3.2 先行研究の課題と本研究の LiDAR 特性を考慮した提案

本研究では、赤外線カットフィルムを用いた物理的偽装攻撃を想定し、LiDAR 点群を欠損させることによる車両検出への影響について検証する。深津らの研究における物理的偽装攻撃の手段として用いる赤外線カットフィルムは本研究においても現実的な手段であると考え、赤外線カットフィルムは LiDAR モデルへの直接的な攻撃ではないため、Cao らや Tu らの課題である、LiDAR の個体差や対象までの距離などの物理的な要素を考慮せずに済む。よって、本研究でも赤外線カットフィルムを車両に貼付し、車両の点群データを欠損させる物理的偽装攻撃を想定する。

深津らの研究では検出対象を車両の背面のみとしているが、将来の自動運転社会においては自動運転車が不特定多数のあらゆる走行環境下で認識を行う必要があり、それは車両背面のみの認識にとどまらない。判定根拠の可視化に関する実験を行った黒木ら [5] の研究では、自車両に近い部分の面において重要度判定が強く反応しているということが明らかにされている。これより、車両の背面ではなく、側面の点群データを検出器が重要としている場合に偽装攻撃を行うときの有効範囲を検証する必要があると考える。そこで、本研究ではそのような車両周辺のあらゆる走行環境を考慮し、車両側面を検出対象に追加する。

以上から本研究では、点群欠損による車両検出に及ぼす影響評価を車両側面を検出対象として検証を行い、物理的偽装攻撃の有効性を検証する。また、PointPillars 検

出器を用いて加工点群を検出するためのフレームワークを提案する。

3.3 本研究の手順

1. 点群データを取得。
2. データ上の点群情報から点群データを書き換え、複数のパターンの欠損を伴う点群データを作成。
3. 作成した点群データを物体検出モデルで検出。
4. 検出結果から、車両側面における最小に近い点群除去範囲を算出。

3.4 データセット

本研究では、KITTI データセットを使用する。KITTI データセットとは、カールスルーエ工科大学と豊田工業大学シカゴ校のグループが公開しているデータセットで、物体認識など自動運転に必要なタスクのベンチマークも提供していて、現在も広く利用されている。表 2 に本研究で使用するデータを示す。

表 2: 使用するデータセット一覧

名前	説明
data_object_calib	カメラパラメータ
data_object_image_2	撮影画像
data_object_label_2	bounding box の位置
data_object_velodyne	LiDAR のセンサデータ (直交座標と反射強度)

3.5 物体検出モデル

本研究では、物体検出モデルとして PointPillars[6] を選択した。PointPillars とその他の物体検出モデルの性能比較を図 2 に示す。

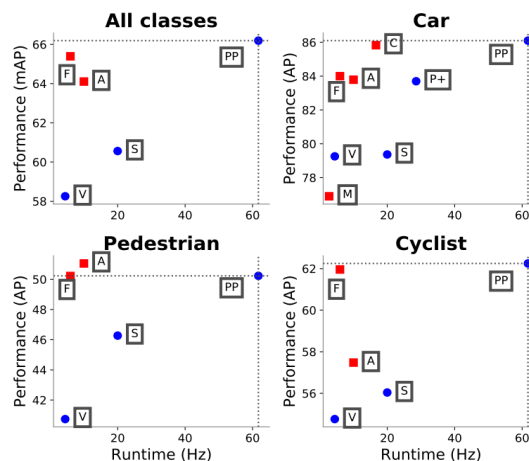


図 2: PointPillars の性能比較 [6]

PointPillars では、VoxelNet や SECOND と異なり、特徴量の抽出が Voxel 単位ではなく Pillar と呼ばれる柱状領域単位で行われる。この Pillar では、高さ方向の分割を行わずにまとめて取り扱うため、Voxel 単位の処理よりもデータ量・計算量を削減することが出来る。そして、

得られた特徴を pseudo-image と呼ばれる特徴に変換し、通常の二次元画像と同様に扱えるようにした上で、2次元の CNN と物体位置検出手法の一つである SSD を利用することで物体検出を行う。

PointPillars の特徴は、物体検出における処理速度と予測精度の両者が優れている点である。予測精度は他の物体検出アルゴリズムと比べ高水準であり、処理速度も従来手法と比べ最も早く動作するアルゴリズムであるとされている。よって、物体検出に関する数多くの論文で積極的に用いられる手法であるため、本研究でも PointPillars を採用する。

4 点群欠損による車両検出への影響評価の実験

4.1 実験環境の構築

本研究では、Windows のコマンドプロンプトを用いて行う。PointPillars の環境構築を GitHub¹を参照し行った。使用したフレームワークとそのバージョンを表 3 に示す。

表 3: フレームワークとバージョン

フレームワーク	バージョン
Numba	0.58.1
Numpy	1.26.1 (学習時), 1.23.0 (検出時)
Open3D	0.17.0
Opencv.Python	4.5.5.62
PyYAML	6.0
setuptools	68.2.2
Torch	2.0.1+cu117
tqdm	4.62.3
TensorFlow	2.09

入力を KITTI データセットの 4 つのファイル (4.1 節の表 2) とし、出力としては AP 値で評価指標を表示し、また、Car, Cyclist, Pedestrian, Van などの自動車、歩行者、自転車のクラス分類、位置を出力する。

Windows での環境構築完了後に、学習の評価を行った。精度がそれぞれ車：90 % 弱、歩行者：50 % 弱、自転車：60 % 強となり、従来通りの精度を達成していた。

4.2 対象点群データの作成

実験で使用する点群データを作成する。まず、KITTI データセットからひとつのシーンの画像データと LiDAR 点群データ (bin ファイル) を選択する。そして、この点群データの中から車両の点群データを抽出する。その際に Open3D というツールを用いる。Open3D は 3 次元データに関する種々な機能を Python, C から扱うことができるソフトウェアである。本研究では、Jupyter Notebook 上に構築した Open3D 環境で実装した。選択した KITTI データセットの点群データの中から Open3D を用いて車両の点群データを抽出する。

このとき、最終的に検出を実装する段階に至るまでに、ファイル形式の変換作業が必要となる。ファイル形式の変換フローを図 3 に示す。

Open3D で取り扱えるファイル形式には、xyz, pcd, ply ファイルなどがあり、一方で取得した KITTI データセッ

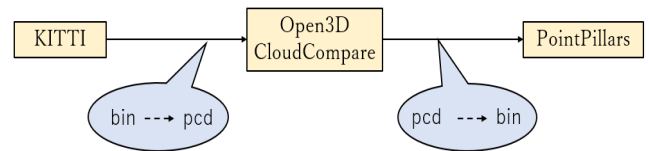


図 3: ファイル形式の変換フロー

トの点群データは bin ファイルであるため、これを pcd ファイルに変換する必要がある。ファイル変換のプログラム構築を GitHub²を参照し行い、ファイル変換を実装した。

変換した pcd ファイルの点群データから、検出対象として車両の点群データを抽出する。そのため、直方体に点群データを切り抜くプログラムを実装した。次に、抽出した車両側面の点群データに欠損を施す加工を行う。点群データの編集は CloudCompare を使用する。CloudCompare は Windows, Mac, Linux で使用できる無償のソフトウェアで、点群データを読み込み、編集することができる。CloudCompare では、インポート可能な 3D データとして pcd ファイル形式があり、書き出しも pcd 形式で行うことができる。そのため、前段階の open3D で取り扱えるファイル形式との互換性を考慮し採用した。また、本研究で使用する PointPillars 検出器では bin もしくは ply のファイル形式でのみ入力が可能である。そのため、編集した点群データを検出する際に、bin ファイルに再変換する必要がある。

4.3 実験結果

KITTI のテストデータ No.000091 (図 4) を検出対象とした。5.2 節で述べた手順で点群欠損を施し、車両側面の点群データの検出を行った。検出結果を図 5 に示す。図中右側の点群欠損範囲については、青色が残した点群を、赤色が除去した点群を示している。尚、車両が検出された際、車両の bounding box に歩行者の bounding box が一部被る検出結果が出力されることがある。本研究では、構築した PointPillars 検出器の検出精度が歩行者の方が車両よりも低いいため、歩行者の信頼度が低いとしてこれを無視できるものと捉える。

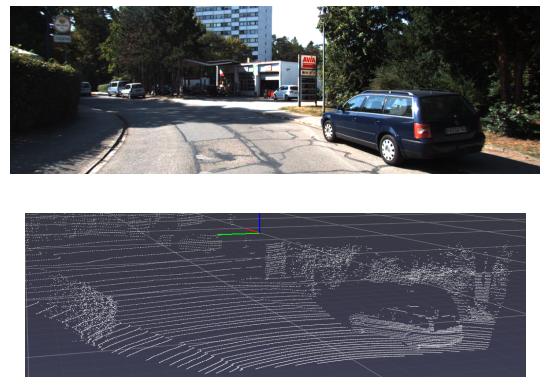


図 4: 検出対象 (上: カメラ画像 下: 点群データ)

¹<https://github.com/zhulf0804/PointPillars>

²<https://gist.github.com/HTLife/e8f1c4ff1737710e34258ef965b48344>

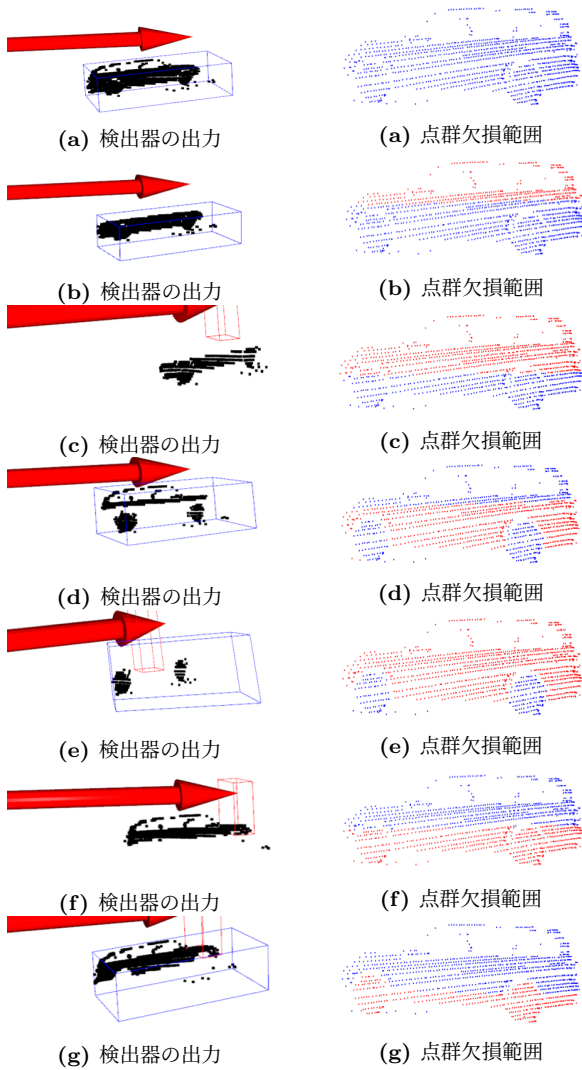


図 5: 検出結果

5 考察

実験結果より、(c)、(f) の点群欠損パターンのときに車両検出が不可になった。よって、最小の点群欠損範囲は、(f) の車両側面下部約 38 % の範囲である。先行研究でも車両背面下部の点群欠損の際に車両検出不可となっていることから、妥当性のある結果だと考える。

ここで、本研究では物理的偽装攻撃の手段として赤外線カットフィルムを車両に貼付し使用する想定であり、タイヤ部分への使用は難しいと考えた。(d)において、側面上部とタイヤの形状に沿った点群では、車両検出が可能であった。そのため、車両側面に対する物理的偽装攻撃を行う際に、タイヤ部分の点群を除去しない場合の最小の点群欠損範囲は(c)の上部約 65 % である。一方で、仮にタイヤ部分の点群データを除去できたとすると、(f) の下部約 38 % の点群を欠損させればよく、比較的容易に物理的偽装攻撃が成り立つと考えられる。しかし、現実的にはタイヤへの細工は難しく、やはり前者の(c)の上部約 65 % の点群欠損が必要となり、側面への物理的偽装攻撃は難しいと考えられる。

以上から、車両側面への物理的偽装攻撃が成立するに

表 4: 検出結果詳細

	検出	点群数 (個)	欠損率 (%)
(a)	可	1347	0
(b)	可	994	41.10
(c)	不可	552	65.74
(d)	可	656	52.13
(e)	bb ズレ	243	86.73
(f)	不可	721	38.75
(g)	可	939	24.97

は約 60 % の範囲に対する細工が必要となり、先行研究での車両背面の約 15 % に比べて難易度が高くなるということが言える。したがって、現実的には車体側面の広範囲に細工を施す必要があるため、LiDAR 検出器を欺く物理的偽装攻撃は、車両側面に関しては不可能に近いということが言える。

6 まとめ

物理的偽装攻撃を想定し、車両側面の検出への影響を検証した。その結果、側面下部のタイヤの高さまでの点群を 40 % 欠損させることで、車両検出が不可となることを明らかにした。しかし、現実的にはタイヤ部分への細工が困難であるということから、上部 60 % の欠損を施す必要があり、車両側面に関しては物理的偽装攻撃は不可能に近いということが判明した。

参考文献

- [1] Yulong Cao et al., “Adversarial Sensor Attack on LiDAR-based Perception in Autonomous Driving,” CCS ‘19: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, pp.2267-2281, November 2019.
- [2] James Tu et al., “Physically Realizable Adversarial Examples for LiDAR Object Detection,” IEEE/CVF Conference on CVPR, pp.13716-13725, 2020.
- [3] 深津 勇貴 et al., “LiDAR ベース物体検出に対する物理的偽装攻撃とその実証,” 電子情報通信学会, 信学技報 vol.121, no.413, HWS2021-81, pp.158-163, March 2022.
- [4] MarketsandMarkets, “自動車用 LiDAR の世界市場”, MarketsandMarkets, November 24 2022, <https://www.gii.co.jp/report/mama1163985-automotive-lidar-market-by-technology-solid-state.html>, 2023.
- [5] 黒木理宏 et al., “自動運転での点群を用いた AI 物体検出における判定根拠の可視化,” 自動車技術会論文集, 53 巻, 4 号, pp.802-807, 2022.
- [6] Alex H.Lang et al., “PointPillars: Fast Encoders for Object Detection from Point Clouds,” IEEE/CVF(CVPR), December 2018.