

令和 4 年 6 月 16 日現在

機関番号：52601

研究種目：基盤研究(C) (一般)

研究期間：2019～2021

課題番号：19K12177

研究課題名(和文)環境センシングのためのセンサセキュリティに関する研究

研究課題名(英文)Research on sensor security for environmental sensing

研究代表者

富沢 哲雄 (Tomizawa, Tetsuo)

東京工業高等専門学校・機械工学科・准教授

研究者番号：60549707

交付決定額(研究期間全体)：(直接経費) 3,400,000円

研究成果の概要(和文)：本研究では、自律ロボットに搭載された外界センサに起こりうる様々な汚損リスクを考慮し、それらが計測データや行動決定に及ぼす影響を調査・分析することで、センサのハードウェアを改変することなくセンサ汚損の有無を検知する手法と、安全を担保するための適切な対応策を示すことを目的とした。3年間の研究により、センサ周囲の移動物体を継続的に観測しながら、その際に得られる受光強度の時間的変化パターンを統計処理することにより、センサ投受光部の汚損を検出したり、汚損による光の減衰率を推定して本来の情報を復元する手法を確立することに成功した。

研究成果の学術的意義や社会的意義

自律移動ロボットや車の自動運転システムは、センサで観測した環境情報に基づいて行動を決定している。そのため、これらのシステムに搭載されたセンサの計測部に何らかの汚損等が発生し、正しい情報がシステムに入力できなくなった場合には、設計者が意図していない動作が引き起こされ、重篤な事故が発生する危険性をはらむ。

本研究は、ハードウェアを改変することなく、計測データを統計処理することにより、リスク要因となる汚損を検出するとともに、汚損した状態であっても一定期間にわたりシステムを安全に運用するためのアルゴリズムを提案しており、自動化システムの信頼性向上に貢献するものである。

研究成果の概要(英文)：Dirt on the optical lenses of sensors mounted on autonomous robots can be a source of fatal noise.

The objective of this study was to detect the presence of sensor contamination without modifying the sensor hardware and to indicate appropriate countermeasures to keep the system safe.

Through three years of research, we developed a method to detect contamination of the optical lens of the sensor by continuously tracking and observing moving objects around the sensor. Furthermore, we established an algorithm to recover the original information by estimating the rate of light attenuation due to contamination.

研究分野：ロボット工学

キーワード：センサセキュリティ LiDAR 光学レンズ汚損 ロボット

1 . 研究開始当初の背景

ロボットや IoT 技術の発展にともない、近い将来、人間社会の中には無数のセンサを搭載したロボットシステムやデバイスが溶け込んでくることが想定される。これらのシステムは、周辺環境を観測して膨大な情報を集め統計的な処理をすることで有用な情報を抽出し、社会や環境に対して物理的に作用を加えるという性質を持つ。特に近年は、自動車や介護の分野などで人間にとって負担の大きい作業を自動化しようとする試みが盛んに行われている。人間と物理的に接する機会の多い自動化システムが万が一誤動作を起こすと、人命に関わる重篤な事故につながる可能性がある。

従来のロボット工学分野では、物体認識・自己位置推定・障害物回避・ヒューマンインターフェイスなどの要素研究は盛んに行われてきたが、これらは基本的に『センサは安全に保たれている』という前提に基づいて設計されているものであり、自身のセンサの安全性を担保する手法に関する研究例は見られなかった。センサに生じる誤差を確率的なモデルとして表現する手法は一般的に利用されているものの、未知の汚損により特性が変化する場合には対応できない。我々は、ここに完全自律化の実現に向けて理想と現実の間に大きなギャップが存在すると考えている。今後、より信頼性の高いシステムを実現するためには、情報の入口であるセンサの安全性を確保するセンサセキュリティ技術が非常に重要となってくる。近年の市販のセンサには、汚れを検出するための追加センサを備えた製品も登場しているが、検出できる異常の種類は限定的であり、またハードウェアの変更を必要とするため、既存のセンサをすべて置き換えることは容易ではないことから、ハードを改変することなくシステムの安全性を強化する手法が望まれている。

2 . 研究の目的

ロボットが周囲の環境を観測するために用いられる外界センサは、その性質上、計測素子やレンズ、およびそのカバーが外部に露出する形で設置されていることが多い。そのため、センサの計測部は天候や振動衝撃に起因する偶発的な汚損や人為的攻撃によるノイズに晒されるリスクを持っている。

本研究では、近年のロボットシステムで広く採用されているレーザー距離センサ (LiDAR) を対象とし、光学レンズの一部に汚れが付着している場面を想定する。観測値を統計処理することで、汚損が生じた範囲を特定するとともに、汚損によりノイズを受けた計測値を、正しい値に復元する手法を明らかにすることを目標とした。



実験に使用したセンサと汚損を模擬した減光フィルム

3 . 研究の方法

一般的な LiDAR は、円筒型あるいはドーム型の外側レンズをもち、その内部にレーザー光を投受光するユニットが組み込まれている。機械的にユニットを回転・揺動させることで、外側のレンズを通して周囲の様々な方向にレーザー光を照射している。本研究では、外側レンズに付着しやすい埃や泥水を模倣して、レンズの一部に様々な減光フィルムを貼り付け、これらの影響を調査するとともに、フィルムを貼り付けた場所を特定し、またその減衰率を推定することとした。

次に、汚損箇所を特定する基本的なアイデアについて述べる。計測のために照射されるレーザー光の光路のレンズが汚れていると、その影響でレーザー光に一定の減衰が生じ、受光する光の強度が下がる。LiDAR は先に述べたように内部のユニットが回転しながら、様々な方向に向けてレーザーを照射するため、外側レンズの一部に汚れが付着していると、その方角の計測値にのみ減衰の影響が表れる。そこで本研究では、特定の物体とセンサとの相対位置を徐々に変化させながら、レンズの様々な部位を通して同一物体を一定時間観測し続け、特定の方向で顕著な受光強度の減衰が見られるかどうか分析することで、外側レンズの汚損を検出する。また、汚損が無い部分と汚損がある部分で同一物体の見え方がどの程度変化するか分析することで、汚損の程度 (減衰率) を明らかにできると考えた。汚損による減衰率を推定することができれば、そこから本来の受光強度を算出することも可能となる。また同時に、統計的な手法のみならず、機械学習を用いて汚損を検出できるかどうか検討する。

4. 研究成果

(1) 特定の相対運動をする物体を一定時間観測する手法

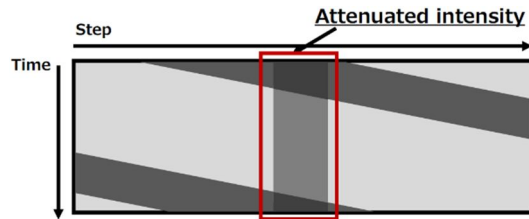
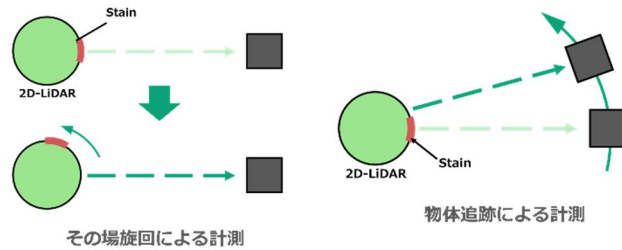
提案手法が正しく機能するか検証するために、センサと特定の物体との相対位置を徐々に変化させながら二次元LiDARのデータを取得し、観測情報の時間的な変化から統計的にレンズ汚損を検出できることを確認した。

具体的には、a) 静的な環境にセンサを置き、センサをゆっくりと等角速度でその場旋回させる方法、b) センサを固定した状態で、センサを中心とする同心円状に特定の物体を移動させ、その物体を追跡する手法の2通りを確かめた。

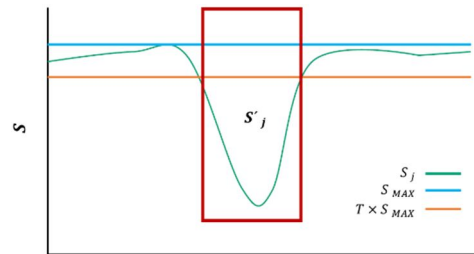
a) のケースにおいては、センサが1度回転するごとに1回の計測を行いながら、一周分=360回のデータを取得し、それぞれの受光強度を画像として出力する方法を採用した。生成された画像を見ると、レンズに汚れがある箇所には矩形上の影が現れる。実験により、減光率20%以上のフィルムを正確に検知することができることを明らかにした。

b) のケースにおいては、特定の物体をトラッキングしながら、その対象物の明るさの変化を観測する。同一物体を追跡しているため、本来はどの方向から見ても同じ明るさで観測されるはずだが、レンズが汚れている部分を通して観測すると、相対的に暗く見える。この仕組みを利用して、a) と同様に汚損を検出できることを明らかにした。

このa) b) の成果は、それぞれSICE SI 部門講演会2019および2020で優秀講演賞を受賞した。



相対姿勢を変化させ一定時間観測を続けたときの受光強度の変化を可視化



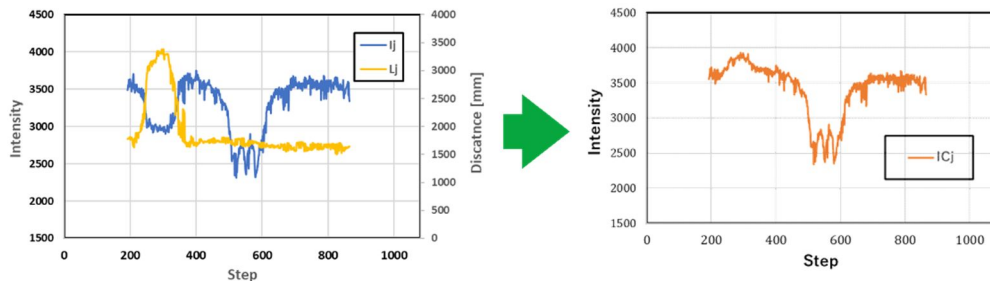
計測データの明るさ分布

(2) センサ周辺に存在する任意の移動物体を一定時間観測する手法

上記(1)は、「静的な環境でセンサをその場旋回させる」あるいは「特定の物体を同心円状に動かす」という特殊な操作が必要であった。本研究では、より簡易的に汚損検出できるようにするために、センサ周辺に存在する任意の移動物体を追跡することで、同様の汚損検出ができるように一般化を図った。

これまででは、センサと対象物との相対距離が一定という前提が使えたが、任意の経路を許すと相対距離が変化することを意味する。同一物体を追跡し続けた場合でも、相対距離が遠くなると受光強度が減衰するため、我々は距離の影響によりどの程度の減衰が生じるかを実験的に求め、距離による減衰の影響を取り除くための補正式を立式した。

この補正式を適用することで、センサの周辺を任意の経路で移動する適当な物体を一定時間追跡し、その物体から返ってきたレーザー光の強度を分析することで、センサのレンズに付着させた模擬汚損を検出できることが確認できた。

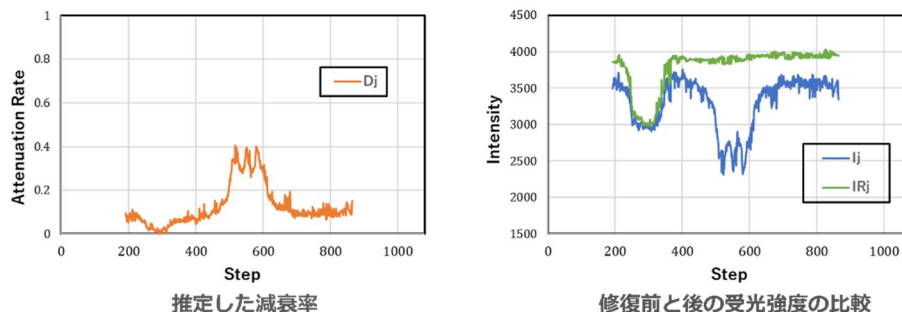


計測結果

距離減衰を補正した受光強度

(3) レンズ汚れによる減衰率推定と元データを復元する手法 (富沢)

上記(2)の方法で得られた受光強度分布から、汚損のある箇所と汚損の無い箇所の明るさの比率を求めることで、レンズの各部分ごとに減衰率を推定することができる。また、それぞれの観測値にその逆数を乗じることで、本来の受光強度を復元できることを確認した。



(4) 機械学習による汚損検出 (三村)

センサへの攻撃を機械学習で検知する手法を検討するにあたり、実環境におけるクラス不均衡問題への新たな対策を検討した。少量の悪性 JavaScript を敵対的生成ネットワークを用いてオーバーサンプリングし、実環境におけるクラス不均衡問題を軽減する手法を検討した。実環境を模して作成したデータセットを用いて評価を実施し、その成果を雑誌論文として投稿中である。

5. 主な発表論文等

〔雑誌論文〕 計2件（うち査読付論文 2件 / うち国際共著 0件 / うちオープンアクセス 1件）

1. 著者名 Ngoc Minh Phung, Mamoru Mimura	4. 巻 -
2. 論文標題 Oversampling for Detection of Malicious JavaScript in Realistic Environment	5. 発行年 2020年
3. 雑誌名 Advances on Broad-Band Wireless Computing, Communication and Applications	6. 最初と最後の頁 176-187
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-61108-8_17	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 -

1. 著者名 Ngoc Minh Phung, Mamoru Mimura	4. 巻 13
2. 論文標題 Detection of malicious javascript on an imbalanced dataset	5. 発行年 2021年
3. 雑誌名 Internet of Things	6. 最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.iot.2021.100357	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 -

〔学会発表〕 計5件（うち招待講演 0件 / うち国際学会 1件）

1. 発表者名 森本大志, 富沢哲雄, 岩切宗利
2. 発表標題 追跡物体に関する時系列パターン解析による測域センサ汚損検出
3. 学会等名 第21回計測自動制御学会システムインテグレーション部門講演会
4. 発表年 2020年

1. 発表者名 富沢哲雄, 戸島淳
2. 発表標題 時系列パターン解析による測域センサデータの異常検出
3. 学会等名 第20回 計測自動制御学会システムインテグレーション部門講演会
4. 発表年 2019年

1. 発表者名 宮崎裕輔, 李珠熙, ファンアンソン, 坂本徹, 東滲, 押部樹希, 林周瑚, 富沢哲雄
2. 発表標題 初めて訪れた屋内環境における自律移動に関する研究
3. 学会等名 第20回 計測自動制御学会システムインテグレーション部門講演会
4. 発表年 2019年

1. 発表者名 菅裕弥, 三村守
2. 発表標題 実環境におけるParagraph Vectorを用いた悪性JavaScriptの検知手法
3. 学会等名 第61回計測自動制御学会システム工学部会研究会資料
4. 発表年 2019年

1. 発表者名 Mamoru Mimura, Yuya Suga
2. 発表標題 Filtering Malicious JavaScript Code with Doc2Vec on an Imbalanced Dataset
3. 学会等名 The 14th Asia Joint Conference on Information Security (国際学会)
4. 発表年 2019年

〔図書〕 計0件

〔産業財産権〕

〔その他〕

-

6. 研究組織

	氏名 (ローマ字氏名) (研究者番号)	所属研究機関・部局・職 (機関番号)	備考
研究 分担 者	岩切 宗利 (Iwakiri Munetoshi) (00535362)	防衛大学校(総合教育学群、人文社会科学群、応用科学群、 電気情報学群及びシステム工学群)・電気情報学群・准教授 (82723)	

6. 研究組織（つづき）

	氏名 (ローマ字氏名) (研究者番号)	所属研究機関・部局・職 (機関番号)	備考
研究 分 担 者	三村 守 (Mimura Mamoru) (60815017)	防衛大学校（総合教育学群、人文社会科学群、応用科学群、 電気情報学群及びシステム工学群）・電気情報学群・准教授 (82723)	

7. 科研費を使用して開催した国際研究集会

〔国際研究集会〕 計0件

8. 本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関