様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　３ 年　 ６ 月 １０ 日現在

機関番号：３４３１５
研究種目：基盤研究(C)（一般）
研究期間：2018～2020
課題番号：１８Ｋ１１３０８

研究課題名（和文）車載応用に向けた耐タンパセキュアセンシングシステムの研究

研究課題名（英文）Tamper resistant secure sensing system for vehicle applications

研究代表者
藤野　毅（FUJINO, TAKESHI）

立命館大学・理工学部・教授

研究者番号：６０３６７９９３

交付決定額（研究期間全体）：（直接経費）　　3,300,000円

研究成果の概要（和文）：周囲の物体を測距センサ等で検知して衝突を回避するための運転者への警報通知や，さらにブレーキやアクセル，ハンドルを自動制御するシステムなどが，自動車運転支援システムとして近年実用化されている．このようなシステムの安全性を高めるためには，周囲の物体を正常に検知することが必須であるが，近年外部から物理的な攻撃を行い，センサの値を測定不能または改ざんするような手法が学会で発表されている．このような攻撃を回避するための「耐タンパセキュアセンシングシステム」の研究を行った．

研究成果の学術的意義や社会的意義
研究では，超音波測距センサを用いて，計測の不能化や計測値の改ざんなどの攻撃が可能であることを実証した．これに対して，センシングする超音波の波形処理や時系列情報を用いて攻撃を検知する耐タンパセンシング手法の研究を行った．また，可視光・赤外線イメージセンサを用いたセンサフュージョンの研究・LIDARを用いた自己位置推定や地図作成を行う際の攻撃手法の研究も行い，学会発表等を通じて学術に貢献した．
これらの研究成果は，車載応用だけでなく，センサをもちいて周囲の情報を取得し動作を判断するような，さまざまな機器（ロボット等）での応用が期待でき，広範な社会で使用される機器の安全性・信頼性の向上が期待できる．

研究成果の概要（英文）：Recently, advanced driver assistance systems (ADAS) have begun to be practical use, which detect surrounding objects by range sensors, and notify the driver of warnings to avoid collisions, as well as systems that automatically control the brake, acceleration, and steering. In order to increase the safety of such systems, it is essential to detect surrounding objects properly. However, a method to disable or falsify sensor values by physical attacks from outside has been presented in academic conferences in recent years. In order to avoid such attacks, we conducted research on a "tamper-resistant secure sensing systems".

研究分野：ハードウェアセキュリティ

キーワード：センサセキュリティ　計測セキュリティ　測距センサ　遠赤外線カメラ　超音波センサ　LIDAR

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

2021 年現在普及が進んでいる，先進運転支援システム（ADAS：Advanced Driving Assistant System）においては，図１に示すような，様々なセンサを用いている．完全自動走行車においては，これらに加えて全方位 LIDAR（Laser Imaging Detection And Ranging）と呼ばれるセンサが搭載される見込みである．

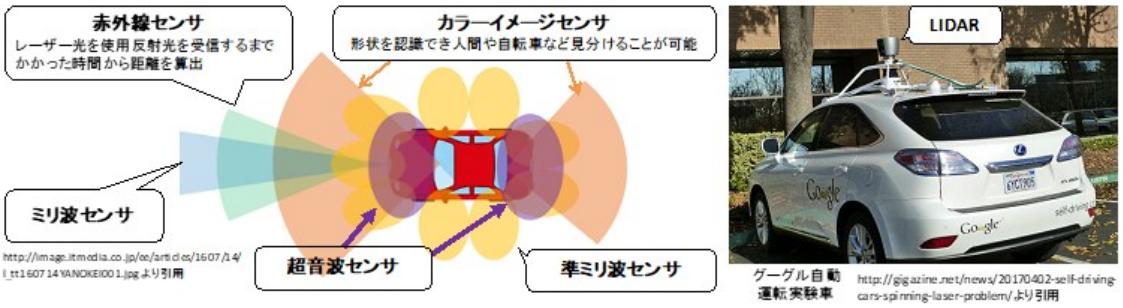


図１．先進運転支援システムを搭載した自動車に搭載される各種センサ(左）と LIDAR(右)

一方で，センサがデータセンシングする際の物理攻撃手法は 2014 年から海外の学会で発表が始まっていたが，本研究開始前に我々の研究グループでは，2016 年１月に世界で初めて，超音波センサに対して，外部から超音波を照射することにより測距不能とする，または測距値を実際値よりも短く改ざんする攻撃を報告した．図２に，研究開始当時に車載センサに対する攻撃に関連する国内外の研究成果の発表をまとめた．左側から３つ目の超音波ソナーが我々の発表である．攻撃事例自体もまだ少なく，対策技術の発表事例は，2017 年当時存在しなかった．

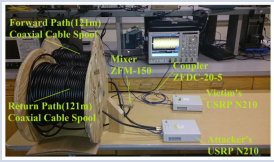
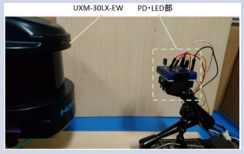
ミリ波レーダー	カメラ/LIDAR	超音波ソナー	LIDAR
			
ユタ州立大学	Security Innovation社	立命館大学/三菱電機	横浜国立大学
Ruchir Chauhan, Ryan M. Gerdes and Kevin Heaslip, “Demonstration of a False-data Injection Attack Against an FMCW Radar,” ESCAR Europe 2014	. Petit, B. Stottelaar, M. Feiri, F. Kargl, “Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR,” Black Hat Europe 2015	中澤祐希，中野将志，汐崎充，久保田貴也，白畑正芳，藤野毅，菅原健，鈴木大輔，小林信博，“車載測距センサに対するセキュリティ評価,” SCIS2016, January 2016	相馬一樹，藤本大介，松本勉，“あるパルスLIDARシステムの反射光偽装に対する計測セキュリティ”，IEICE，2016，5月

図２．車載測距センサに対する物理的攻撃事例（2017 年まで）

２．研究の目的

研究の背景で述べたように，センサに対して関して，物理攻撃によって測定値が改ざんすることが可能である．自動車の ADAS を構成している測距センサが物理攻撃を受け測距出力が改ざんされると，運転支援制御の誤動作を誘発し安全走行に対する重大な脅威となる．このため本研究では攻撃に対する対策技術を提案し，実際にセンサを用いてその効果を実証することを目的とした．

３．研究の方法

本研究では当初計画として以下(1)～(3)の 3 つの手法で研究を進めた．研究を進めていく段階で，上記の研究目的に一致する研究として新たに(4) (5)のテーマも実施した．

(1)タイムオブフライト(ToF)方式測距センサにおける耐タンパ測距手法

センサ自身が発生した超音波と，攻撃用超音波スピーカーが発信した超音波を区別することができる手法を提案し，その効果を検証する．

(2)センシング値の時系列変化を用いた攻撃検知

センサを用いて，連続センシングしている際の測距値や速度を深層学習技術を用いて学習することで異常値が測定された場合に攻撃を検知する手法を検討し，その効果を検証する．

(3)異種のセンサを用いたセンサーフュージョン

赤外線カメラと可視光カメラという 2 つの画像や，超音波センサと LIDAR といった異種のセンサからの出力を,深層学習技術を用いて，高精度にセンシングする技術を構築し，同時に悪意ある攻撃に対する耐性を検証する．

(4)CMOS イメージセンサのフリッカノイズで画像認識を困難にさせる攻撃の研究

車載カメラなどで使用されている CMOS イメージセンサに対して，LED 照明によって照度変化をおこなうことでフリッカノイズを発生させ取得した画像に縞模様を発生させることで物体認識を困難にさせる攻撃手法の研究を行う．

(5)LIDAR の測距値の改ざんすることで自己位置推定およびマップ作成を改ざんする研究

LIDAR は赤外線を使って自車周囲の状況を把握することができる，自動運転実験車では必須の測距センサであり，自己位置推定やマップ作成に使用されている．このセンサに対する測距値改ざん攻撃事例は，図２に示したように他の研究機関により実施されているが，本研究では測距値の改ざんが自己位置推定やマップ作成といった後処理に対してどのような影響を与えるかを調査する研究を行う．

４．研究成果

(1)タイムオブフライト(ToF)方式測距センサにおける耐タンパ測距手法

【2018 年度】

センサ送信部において発生する超音波に対して，攻撃者が送信間隔を予測できない２種類のランダムパルスを送信する手法の研究をおこなった．センサ自身が発生した信号と受信波との相関を求め，相関の高くない受信波を得た時には攻撃波であると判断する手法を用いて，耐タンパ測距手法を実現した．成果を 2019 年 3 月の国際会議で"Study of Ultrasonic-Range-Sensor System with Resistance to Spoofing Attack"というタイトルで発表した．

(2)センシング値の時系列変化を用いた攻撃検知

【2018 年度】

超音波測距センサおよび本研究費で購入した LIDAR の測距値の時系列変化を入力として，カルマンフィルタによって次時刻の測距値を予測し，攻撃を検知する手法の実測による検証を行なった．また，２種類の測距センサの値が異なる時に,「信頼度」を用いて攻撃を回避する新たな手法を提案した．成果を 2019 年 3 月の国際会議で"Study of Countermeasure Using Time-Series Data against Physical Spoofing Attack on Range Sensor"というタイトルで発表した．(図３)

自動車の車速のようにアクセルやブレーキによって車速が連続的に変化する値は，過去の車速とアクセルやブレーキ量によって深層学習を使った予測が可能となる．この手法を

2018 年 6 月の国内学会で「車載ネットワークにおける深層学習を用いた時系列解析による攻撃検知手法」というタイトルで発表した．さらに，この研究をすすめて，自動車の速度計表示を改ざんする攻撃がなされた際に，小型組み込み電子機器である RaspberryPi を用いて正しい表示を行えるデモシステムを開発し，2019 年 1 月の国内学会で「深層学習を用いた時系列予測による車載ネットワーク攻撃検知手法の実車環境への適用評価」というタイトルで発表した．（図４）

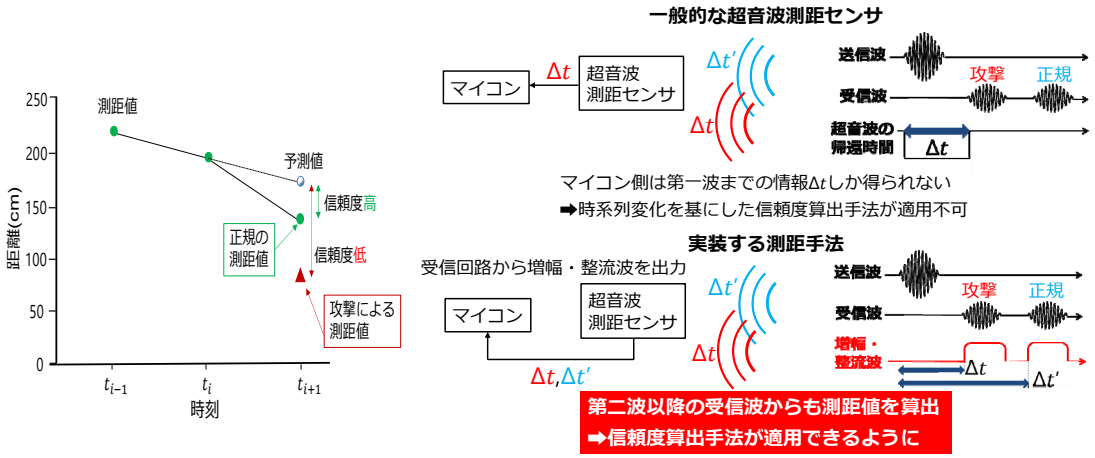


図３．測距値の時系列変化を用いて信頼度を算出する超音波測距センサシステム

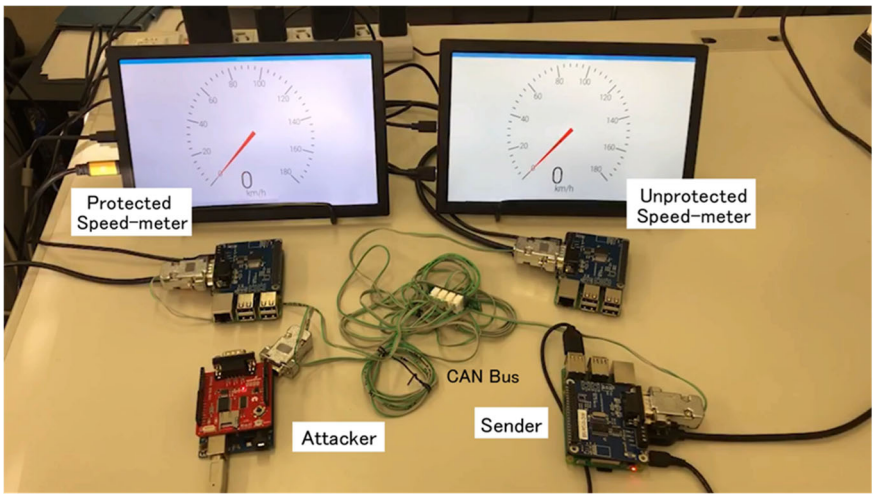


図４．深層学習を用いた自動車の車速異常検知システムの実証動作デモシステム

【2019 年度】

2018 年の自動車の車速予測検知は，時系列の深層学習ネットワークである RNN をもちいて車速を予測し，実際の車速が予測値と大きく異なった場合に攻撃を検知する手法をとったが，新たな深層学習手法として AutoEncoder を用いて，攻撃検知をより高精度に行う手法を開発した．本成果を 2019 年５月の国内会議で「AutoEncoder を用いた車載ネットワークへのなりすまし攻撃検知手法の提案」というタイトルで発表した．

(3) 異種のセンサを用いたセンサーフュージョン

【2018 年度】

可視光カラーイメージセンサと遠赤外線画像センサを用いて画像を同期して撮影するシステムを構築した．このシステムを自動車のルーフに搭載して撮影を行い，２種類の画像を用いたディープラーニングによるセンサフュージョンで夜間でも人物の認識精度が向上することを確認した．成果を 2018 年６月の国内会議で「深層学習技術を用いた RGB-FIR カメ

ラセンサフュージョンによる車載向け物体認識」というタイトルで発表した.（図５）

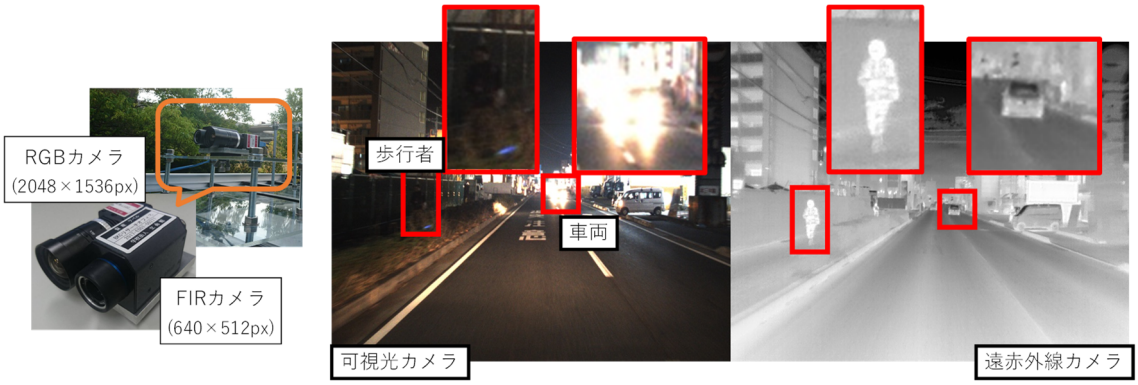


図５．可視光カラーイメージセンサと遠赤外線画像センサを用いたセンサーフュージョン

【2019 年度】

本研究サブテーマの内容は出版社からの執筆依頼を受け，2020 年 3 月 10 日にシーエムシー出版から発行された書籍「自動運転・運転支援の実現に向けたセンサ開発」の「第 5 章深層学習技術を用いた RGB-FIR カメラセンサフュージョンによる車載向け物体認識」として掲載された.

(4)CMOS イメージセンサのフリッカノイズで画像認識を困難にさせる攻撃の研究

【2018 年度】

CMOS イメージセンサに発生させることのできるフリッカ・ノイズパターンをシミュレーションし，画像認識ソフトウェアにおいて人物の認識機能が低下することを確認した．本研究成果は，2018 年９月の国内会議で「カメラに対するフリッカ・ノイズを用いた人物検出の妨害」というタイトルで発表した．さらに，様々な光源の点滅の周期，点灯/消灯の明るさ比，時間（Duty）比を制御できる照明を使用して実際にフリッカを発生させる実験を行い，実環境においても攻撃が成功することを確認した．本成果は，2019 年３月の国内会議で「フリッカ・ノイズを用いた歩行者検出システム妨害手法の検討」というタイトルで発表した.

(5)LIDAR の測距値を改ざんすることで自己位置推定およびマップ作成を改ざんする研究

【2020 年度】

自動車などの移動物体に搭載された LIDAR に対して，複数の角度からの測距値を改ざんすることにより，LiDAR-based SLAM の自己位置推定を騙す攻撃手法を提案し，2020 年 7 月の国内会議で「LiDAR-based SLAM における姿勢推定のための ICP アルゴリズムに対する敵対的スキャン生成攻撃」として発表した．さらに，連続して姿勢の改ざんを行うことで，SLAM によって生成される地図が異常となることを，2021 年１月の国内会議で「LiDAR-based SLAM に対する敵対的スキャン生成攻撃と生成地図への影響評価」で発表した.

５．主な発表論文等

〔雑誌論文〕　計0件

〔学会発表〕　計11件（うち招待講演　1件／うち国際学会　2件）

１．発表者名 青砥　光志，吉田　康太，汐崎　充，久保田　貴也，白畑　正芳，藤野　毅
２．発表標題 AutoEncoderを用いた車載ネットワークへのなりすまし攻撃検知手法の提案
３．学会等名 LSIとシステムのワークショップ2019
４．発表年 2019年

１．発表者名 吉田康太，飯田啄巳，橋本匠，汐崎充，白畑正芳，久保田貴也，藤野毅
２．発表標題 深層学習技術を用いたRGB-FIRカメラセンサフュージョンによる車載向け物体認識
３．学会等名 自動車技術会２０１８年春季大会
４．発表年 2018年

１．発表者名 亀岡良太，吉田康太，西村勇人，汐崎充，久保田貴也，　白畑正芳，藤野毅
２．発表標題 車載ネットワークにおける深層学習を用いた時系列解析による攻撃検知手法
３．学会等名 自動車技術会２０１８年春季大会
４．発表年 2018年

１．発表者名 榊原弘貴，吉田康太，汐崎充，白畑正芳，久保田貴也，藤野毅
２．発表標題 カメラに対するフリッカ・ノイズを用いた人物検出の妨害
３．学会等名 電子情報通信学会，ソサイエティ大会
４．発表年 2018年

１．発表者名
玉井晃太郎，亀岡良太，吉田康太，汐崎充，久保田貴也，白畑正芳，藤野毅

２．発表標題
深層学習を用いた時系列予測による車載ネットワーク攻撃検知手法の実車環境への適用評価

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS）2019

４．発表年
2019年

１．発表者名
榊原弘貴，吉田康太，白畑正芳，熊木武志，藤野毅

２．発表標題
フリッカ・ノイズを用いた歩行者検出システム妨害手法の検討

３．学会等名
電子情報通信学会，ハードウェアセキュリティ研究会

４．発表年
2019年

１．発表者名
Yuta Kajitani, Hayato Nishimura, Kota Yoshida, Mitsuru Shiozaki , Takaya Kubota, Takeshi Fujino

２．発表標題
Study of Countermeasure Using Time-Series Data against Physical Spoofing Attack on Range Sensor

３．学会等名
RISP International workshop on Nonlinear Circuit, communications and Signal Processing（国際学会）

４．発表年
2019年

１．発表者名
Hayato Nishimura,Yuta Kajitani, Kota Yoshida, Mitsuru Shiozaki , Masayoshi Shirahata,Takaya Kubota, Takeshi Fujino

２．発表標題
Study of Ultrasonic-Range-Sensor System with Resistance to Spoofing Attack

３．学会等名
RISP International workshop on Nonlinear Circuit, communications and Signal Processing（国際学会）

４．発表年
2019年

１．発表者名
藤野毅

２．発表標題
センサに対する物理攻撃とそれに対する多層的な対策手法

３．学会等名
IEICE 綜合大会　ソサイエティ特別企画（招待講演）

４．発表年
2019年

１．発表者名
吉田　康太，藤野　毅

２．発表標題
LiDAR-based SLAM における姿勢推定のための ICP アルゴリズムに対する 敵対的スキャン生成攻撃

３．学会等名
電子情報通信学会，ハードウェアセキュリティ研究会

４．発表年
2020年

１．発表者名
北條 雅矢，吉田　康太，藤野　毅

２．発表標題
LiDAR-based SLAMに対する敵対的スキャン生成攻撃と生成地図への影響評価

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS）2021

４．発表年
2020年

〔図書〕　計1件

１．著者名	４．発行年
監修： 室　英夫（分担執筆者　吉田康太，藤野毅）	2020年
２．出版社	５．総ページ数
シーエムシー出版	278（執筆ページは9ページ）
３．書名	
自動運転・運転支援の実現に向けたセンサ開発	

〔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

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