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　２ 年　 ６ 月 １２ 日現在

機関番号：１４６０３
研究種目：若手研究
研究期間：2018～2019
課題番号：１８Ｋ１８０５０

研究課題名（和文）計測装置におけるセキュリティ要件の解明と対策技術の開発検討

研究課題名（英文）Fundamental study on security requirements for measuring devices and development of countermeasure technology

研究代表者
藤本　大介（Fujimoto, Daisuke）

奈良先端科学技術大学院大学・先端科学技術研究科・助教

研究者番号：６０７３２３３６

交付決定額（研究期間全体）：（直接経費）　　3,000,000円

研究成果の概要（和文）：本研究は、自律制御システムで外界の情報を取得するセンサデバイスの取得過程におけるセキュリティに関して、センサへの入出力となるアナログ信号に着目し、攻撃可能性の評価、および対策技術の検討を行った。攻撃可能性の評価のために実センサを用いた攻撃再現環境を構築し、その過程において電磁波を通じたセンサの測定タイミングを攻撃者が取得できた際に攻撃範囲が拡大することを明らかにした。また、対策技術としてデジタル信号変調がアナログ信号に変換される過程での非線形性により攻撃者が外部でアナログ信号を取得したとしても再現が困難になる可能性を示した。

研究成果の学術的意義や社会的意義
本研究で得られた知見は、自動運転などの眼となるセンサデバイスに関するものであり、同様の計測原理を持つセンサ全般に応用できる可能性がある。そのため、社会実装が進む自動運転デバイスに対して悪意を持つ攻撃者の攻撃を事前に検討することが可能になり、未然に攻撃を防ぐことに役立つ可能性がある。

研究成果の概要（英文）：In this study, we focused on the analog signals that are input and output to the sensor, and evaluated the attack potential and examined the countermeasure technology regarding the security in the acquisition process of the sensor device that acquires the external information by the autonomous control system. . We constructed an attack reproduction environment using an actual sensor to evaluate the attack potential, and revealed that the attack range expanded when the attacker could acquire the measurement timing of the sensor through electromagnetic waves in the process. In addition, as a countermeasure technology, it was shown that even if an attacker acquires an analog signal externally, it may be difficult to reproduce it due to nonlinearity in the process of converting digital signal modulation into an analog signal.

研究分野：情報セキュリティ

キーワード：ハードウェアセキュリティ　センサセキュリティ　計測セキュリティ

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

近年、多くの情報機器がセンサからの情報をもとに動作している。これらのセンサで取得されたデータは測定エラーなどを除き信頼のおけるものとして扱われている。しかし，悪意のある攻撃者がセンサからの出力値を誤らせたり，計測を不可能にしたりするなどの計測におけるセキュリティリスク（計測セキュリティ）が提案されている。特に自動車においては自動運転に用いられる LiDAR に対する攻撃が提案されており[1], 人命にかかわる脅威として認識されつつある。これらの攻撃はセンサの仕組み自体を狙うものであり，センサの出力データ（デジタルデータ）からでは攻撃を検知することは困難である。様々なセンサに対する攻撃が提案されているが、対策技術については複数の異なる原理で動くセンサを組み合わせるにとどまっている。

２．研究の目的

本研究ではセンサに対する攻撃の検知をセンサによるアナログ・デジタル変換時のアナログ信号部分や、変換時に発生する電源ノイズのアナログ的特性を観察し、攻撃検知が可能であるかを検討することを目的とする。さらに、アナログ信号の観察からセンサ本来の入力信号と攻撃者が攻撃に使用した信号の分離を行い、妨害攻撃や改ざん攻撃に対する対策手法の提案を検討する。

３．研究の方法

本研究では、センサのうち特に自身が信号を出し、その反射を受けとり計測を行うアクティブセンサを主な対象とし、その攻撃耐性を高めることを最終目的とする。計測機器から発せられる信号が対象物に跳ね返る信号の強度や時間変化などのアナログ特性まで含めて観察を行い、攻撃者がセンサに対して行う攻撃信号を受けた際の動作がどのように異なるかを観察し、その差分をもって攻撃されているかの検知に用いることが可能であるかを検討する。これを達成するためにはまず、反射信号が対象物との距離や対象物の特性(色・形状)に対してどのように変化するかを正確に測定することと攻撃信号がセンサに入力された際にセンサ上にどのようなアナログ信号が流れるかを正確に測定するシステムの構築が必要である。攻撃信号は攻撃者のレベル（マイコンを使った安価なシステムから専用信号発生器をつかった高価なシステム）までの広い範囲で検討を行う。そのために信号発生器を用いて攻撃信号を生成し攻撃信号をセンサに入力し、測定を行う。現在のセンサは自身が出力した信号に類する信号が来たかどうかを、強度信号を用いて判断しているのみであるが、外部の信号の特徴を全て利用することが可能である。本研究ではアナログ―デジタル変換の過程で失われる時間変化などの情報を用いて対策を検討する。

４．研究成果

(1) LiDAR などの測定信号を外部に送信するセンサはその測定タイミングを取得されることにより攻撃者が攻撃信号を生成することが可能となる。測定タイミングを得る手法としては測定信号を直接観測することが考えられるが、センサが駆動する際には電力が消費されその結果電磁波が発生する。本研究の成果として機器から発生した電磁波からセンサの測定タイミングが取得可能であることを実験により明らかにした。また、機器から発生する電磁波の強度は機器内部の信号線の実装に大きく依存しており、自動車などのモジュール間をつなぐコネクタにおいてはその緩みによっては漏れ出る電磁波が増大することを明らかにした。センサに対して電磁波からの測定タイミングの漏洩を防ぐためにはセンサ単体だけでなくシステム全体での漏洩の評価が必要であるといえる。

(2) 測定タイミングの漏洩に関しては、機器の設計に大きく依存しているため、通常の設計においても漏洩の脅威がないデバイスが存在する。そのような機器においても信頼のおけない製造ラインや部品を用いた際に攻撃者が悪意のある回路を埋め込んでいた際に漏洩を引き起こすことが可能であることを、実際に回路を作成し実証を行った。この結果より、センサモジュールをつなぐケーブルやセキュリティレベルの求められるモジュールの製造過程での悪意のある回路の混入を検知、排除する技術が必要という知見を得た。

(3) センサに対する攻撃の可能性として、センサ単体だけでなくシステムとして考えた際にはセンサからの出力データの改ざんという可能性も存在する。攻撃者がシステムを分解できないシチュエーションにおいても電磁波を用いることにより非侵襲で改ざんできる可能性がある。本研究においては IC 間の通信路のデジタルデータに着目して、IC の設計で満たす必要のある電磁波耐性以上の電磁波を印加した際に、データの一部が改ざん可能であることを明らかにした。この結果より、複数の IC を接続した際の電磁波耐性の評価が重要であり、セキュリティレベルの高い機器においては電磁波印加を用いた攻撃の可能性を検討する必要があるといえる。

(4) 評価環境を用いて検討した対策手法として、攻撃者が観測することが可能であるアナログ信号からは復元が困難な識別子を埋め込んだ測定信号の検討を行った。図１に示すように測定には通常は均一なパルスを用いる。そのため、測定タイミングを攻撃者が取得した際に容易になりすましを行うことが可能である。一方でパルスの間隔を測定毎に変更し、識別子とすることにより、元のパルス間隔を知らない攻撃者には生成困難な信号を生成することができる。この際、パルス間隔によりどのようにアナログ信号が変化するかは機器の周波数特性に依存するため、アナログ信号から間隔をリアルタイムに得ることは困難である。一方でセンサ側では振幅変化がどのように起こるかをあらかじめ計算し、反射してきた測定信号の振幅変化と照らし合わせて識別すれば良い。本研究では超音波センサを用いて実証を行ったが他のセンサに対しても有効である可能性が高い。

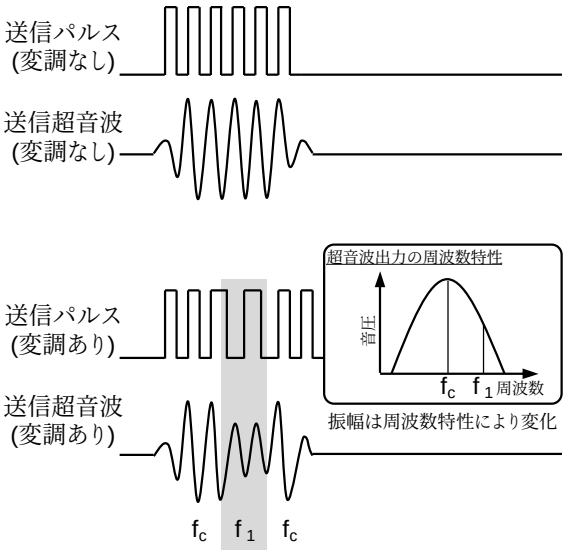

図 1　振幅変調を用いたなりすまし困難化信号

(5) 対策手法で用いる機器毎の識別子は他者から予想されてしまうとなりすまされる危険性がある。そのため、暗号学の分野では乱数を用いることが多い。本研究では、乱数生成に申請乱数生成器を用いることを前提とし、ハードウェア実装を行った際にその乱数性が機器からの漏れ情報により推定可能であるかを検討した。その結果、実装方法に依存して乱数が機器外部から取得可能であることを明らかにした。センサデバイスなどの自律制御機器に組み込まれる場合には機器が外部から取得される脅威を排除するような実装方法及び評価を行う必要性があるといえる。

引用文献

[1] J. Petit, B. Stottelaar, M. Feiri, F. Kargl, “Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR, ”Black Hat Europe 2015, November.2015.

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　0件）

１．著者名 FUJIMOTO Daisuke、NARIMATSU Takashi、HAYASHI Yu-ichi	４．巻 E102.C
２．論文標題 Fundamental Study on the Effects of Connector Torque Value on the Change of Inductance at the Contact Boundary	５．発行年 2019年
３．雑誌名 IEICE Transactions on Electronics	６．最初と最後の頁 636～640
掲載論文のDOI（デジタルオブジェクト識別子） https://doi.org/10.1587/transele.2019EMP0005	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 －

１．著者名 Masahiro Kinugawa, Daisuke Fujimoto and Yuichi Hayashi	４．巻 2019
２．論文標題 Electromagnetic Information Extortion from Electronic Devices Using Interceptor and Its Countermeasure	５．発行年 2019年
３．雑誌名 IACR Transactions on Cryptographic Hardware and Embedded Systems	６．最初と最後の頁 62 -90
掲載論文のDOI（デジタルオブジェクト識別子） https://doi.org/10.13154/tches.v2019.i4.62-90	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13件（うち招待講演　0件／うち国際学会　2件）

１．発表者名 Daisuke Fujimoto, Yuichi Hayashi
２．発表標題 Study on Estimation of Sensing Timing Based on Observation of EM Radiation from ToF Range Finder
３．学会等名 Joint International Symposium on Electromagnetic Compatibility and Asia-Pacific International Symposium on Electromagnetic Compatibility, Sapporo（国際学会）
４．発表年 2019年

１．発表者名 Hikaru Nishiyama, Takumi Okamoto, Kim Young Woo, Daisuke Fujimoto and Yuichi Hayashi
２．発表標題 Fundamental Study on Influence of Intentional Electromagnetic Interference on IC Communication
３．学会等名 the 12th International Workshop on the Electromagnetic Compatibility of Integrated Circuits（国際学会）
４．発表年 2019年

１．発表者名
大須賀彩希，藤本大介，林 優一

２．発表標題
TERO-based TRNGの発振回数の変化から推定可能な出力ビットの評価

３．学会等名
ハードウェアセキュリティフォーラム

４．発表年
2019年

１．発表者名
中尾文香，藤本大介，林 優一

２．発表標題
モータ制御通信へのクロックグリッチ注入の影響に関する基礎検討

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
2019年

１．発表者名
大須賀 彩希，藤本 大介，林 優一

２．発表標題
単純電磁波解析を用いたTERO-based TRNGの出力ビット推定

３．学会等名
暗号と情報セキュリティシンポジウム

４．発表年
2020年

１．発表者名
藤本 大介，中尾 文香，林 優一

２．発表標題
スマートロックに対する電磁波照射を用いた強制的な開錠の脅威

３．学会等名
暗号と情報セキュリティシンポジウム

４．発表年
2020年

１．発表者名
西山 輝，岡本 拓実，藤本 大介，林 優一

２．発表標題
意図的な電磁妨害がIC通信に与える影響に関する基礎検討

３．学会等名
電磁環境両立性研究会

４．発表年
2019年

１．発表者名
藤本 大介

２．発表標題
超音波測距のなりすまし攻撃対策に向けた変調波を利用した振幅制御の検討

３．学会等名
ハードウェアセキュリティ研究会

４．発表年
2018年

１．発表者名
成松 貴

２．発表標題
コネクタのトルク値が接触境界の等価回路に与える影響評価

３．学会等名
環境電磁工学研究会

４．発表年
2018年

１．発表者名
藤本 大介

２．発表標題
Fundamental Study on the Effect of Torque Value at Connector on Equivalent Circuit of Contact Boundary

３．学会等名
機構デバイス研究会

４．発表年
2018年

１．発表者名
藤本 大介

２．発表標題
超音波距離センサから生ずる不要電磁放射計測に基づくセンシングタイミング推定に関する基礎検討

３．学会等名
ハードウェアセキュリティ研究会

４．発表年
2018年

１．発表者名
藤本 大介

２．発表標題
ToF距離センサから生ずる不要電磁放射計測に基づくセンシングタイミング推定を用いた攻撃の検討

３．学会等名
暗号と情報セキュリティシンポジウム

４．発表年
2019年

１．発表者名
成松 貴

２．発表標題
締め付けトルクの減少が接触境界の高周波素子に与える影響に関する検討

３．学会等名
機構デバイス研究会

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