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

平成　３１　年　　４　月　２０　日現在

機関番号：　１７１０２
研究種目：　挑戦的研究（萌芽）
研究期間：　2017～2018
課題番号：　１７Ｋ１９９８４

研究課題名（和文）物理事象空間に基づくサイバーセキュリティ技術

研究課題名（英文）Cyber Security with Physical Characteristics

研究代表者
井上　弘士（Inoue, Koji）

九州大学・システム情報科学研究院・教授

研究者番号：８０３４１４１０

交付決定額（研究期間全体）：（直接経費）　　4,900,000円

研究成果の概要（和文）：無線通信を基本とする組込みシステムにおいて、暗号技術に頼ることなく物理現象を用いたデバイス認証技術を開発した。これにより、無線通信デバイスを対象としたなりすまし攻撃を検知することができるようになる。無線受信信号強度や無線到達時間を用いた認証であるため、攻撃者による改ざんが不可能である。本技術により物理的な空間（範囲）を定義可能となり、今後は様々な応用へと展開することができる。

研究成果の学術的意義や社会的意義
本研究の学術的意義は、サイバー空間をフィジカル（物理）現象を用いて守る、という点にある。基本的に物理現象は改ざん不可能であり、これをより所とすることで、いわゆる攻撃者と防御者のイタチごっこに終止符を打つことができる可能性がある。今後は無線接続されたデバイスを搭載したシステムの普及が予想され、これらに対し本技術を適用することができる。

研究成果の概要（英文）：This research proposed and developed a device authorization technique that exploits radio-propagation characteristics (RPCs). Since it does not depend on information processing such as encryption technology, we can apply it resource-restricted devices such as IoT applications. By using our technique, we can detect spoofing attacks targeting wirelessly communicated devices. The most important feature is that our technique makes it possible to define "physical space" by exploiting RPCs and it can be used for many future applications.

研究分野：　コンピュータ・アーキテクチャ

キーワード：　サイバーセキュリティ　無線通信　組込みシステム

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９、ＣＫ－１９（共通）

１．研究開始当初の背景

様々なデバイスがネットワークで相互接続される IoT 時代の到来が目前に迫ってきた．一般ユーザの日常生活を一変させるのみならず，第 4 次産業革命をもたらすと期待されている．特に，各デバイスの移動可能性を考慮した場合，無線通信を基本とした IoT システムが爆発的に普及することが容易に予想される．このように，相互接続可能性を高めることで新しい社会や産業を構築できる反面，サイバーテロの脅威がより深刻となる．サイバーセキュリティ問題を難しくする本質的な要因は，アクセス可能性がネットワーク空間全域へと広がり，防御すべき物理空間を明確に定めることができない点にある．もしサイバー空間において防御・監視すべき領域を定義できれば，それに特化した様々な対策を施すことが可能となる．

特に，無線通信を用いた攻撃は物理的移動が可能なため，従来の基地局やゲートウェイによる監視・防御では対応することができない．特に，有線通信にはない情報セキュリティの問題が存在する．そのうちのひとつに，遠隔からの無線なりすまし攻撃が挙げられ，その解決が急務の課題となっている．無線なりすまし攻撃とは，悪意のある送信機が本物のふりをして偽のデータを受信機に送信する脅威である．無線なりすまし攻撃を防ぐ方法として，共通鍵暗号方式や公開鍵暗号方式を用いた認証方式が一般的である．しかしながら，共通鍵暗号方式や公開鍵暗号方式を用いた認証方式には問題が存在する．共通鍵暗号方式においては鍵配送時の傍受の危険があり，公開鍵暗号方式はその問題は解消している一方，データの暗号化と復号に膨大な計算量を要するため，汎用コンピュータと比べて小規模なリソースでの動作を要求されるセンサネットワークや IoT システムには適さない場合がある．

２．研究の目的

本研究の目的は，新しいサイバーセキュリティの概念として「物理事象空間」を導入し，物理情報を用いたサイバーフィジカル・セキュアシステム・アーキテクチャを考案することにある．その実現例として，無線通信車載 IoT システムを対象とした成りすまし攻撃検出技術を確立する．これは，無線受信機の配置を工夫して，攻撃可能空間を物理的にシステム内部に閉じ込めるよう設計するものである．これにより，システム外部からの悪意有る無線なりすまし攻撃を物理的に検出できるようになる．さらに，物理事象空間に基づくセキュア IoT システムの設計法を一般化し，組込みシステムのみならず，家庭やビル，工場，都市，地域など，様々な IoT システムへの適用可能性を検討する．そして，仮想空間での情報処理と物理空間でのセキュリティと言った新しい仮想/物理空間インタフェースを再定義することで，サイバーテロ問題を抜本から解決する一つの手段として完成させる．

３．研究の方法

本研究は，コンピュータ・システム・アーキテクチャを専門とする代表者が中心となり，九州大学に所属する無線通信の専門家の協力を得ながら遂行したものである．具体的には以下のように研究を進めた．

1. 無線受信信号強度や無線到達時間の物理情報を用いた攻撃可能空間を定義する．また，定式化によりそのモデリングを行い，なりすまし攻撃を物理的に検出可能な無線通信デバイス間認証技術を確立する．

2. 無線通信実験環境や既存の専用 IC チップ，さらには，電波伝搬シミュレータを利用して，実効的かつ網羅的な攻撃実験を行う．これにより提案方式の有効性を明らかにする．

3. 車載システム（自動車のタイヤ空気圧監視システム）への適用を想定し，提案するデバイス認証技術の安全性評価を実施する．これにより，物理事象空間構想の実現可能性と有効性を明らかにする．

4. 得られた研究結果と知見を整理し，サイバーシステムにおける物理事象空間の定義法を一般化･普遍化する．そして，組込みシステムのみならず，社会インフラとしての IoT システムなど，様々な状況への適用・展開の可能性を論じる．

現在，サイバー空間におけるセキュリティ対策は，暗号化やネットワーク監視，マルウェア検索など，言わば物理的実態を伴わない方法である．これは，情報処理技術によって高度かつ複雑な機能を実装できる反面，ソフトウェア的手段により（改ざんや成りすましなどによって）妨害が可能であることを意味する．これこそが，言わば攻撃と防御の「いたちごっこ」をもたらす本質的な理由である．これに対し，本研究の本質的な狙いは，サイバー空間においてフィジカルなセキュリティ対策を施すことで，自然法則を破らない限り攻撃不可能な状況を作り出すことにある．これは，サイバー空間と物理空間のインタラクションをセキュリティと言う観

点から再定義したものであり，安全指向サイバーフィジカルシステムと捉えることができる．現在のサイバーセキュリティとは一線を画すアプローチであり,極めて挑戦的であると同時に,安全安心な IoT 社会を実現するために必要不可欠となる．

４．研究成果

本研究の主な成果は以下の通りである。

- 攻撃可能空間の定義とモデル化：受信信号強度比，ならびに，信号到来時刻差を利用した攻撃可能空間のモデルを構築した．ここで攻撃可能空間とは，無線なりすまし攻撃が可能な空間のことであり，逆の捉え方をすると，真の送信デバイスが存在し得る物理的空間のことを意味する．これを定めることにより，設計者は「攻撃可能空間内からの無線通信のみを真の通信と判断する」という前提に基づきシステム開発を進めることができる．なお，真の送信機ならびに受信機の配置により撃可能空間の大きさや形状を制御可能となる（例えば，攻撃可能空間をシステム筐体内に設定することで，外部からの攻撃を不可能にする）．

- 電波伝搬シミュレータを構築し，タイヤ空気圧監視システム（TPMS）をケーススタディとした提案手法のセキュリティ評価を行った．真の信号，攻撃者信号それぞれの受信信号強度に生じるノイズを確率モデルによって表現し，各地点からの攻撃可能性を算出した．その結果，複数信号による多数決的な認証手続きを採用することで，攻撃可能空間を対象システム内に限定できることを示した．

- ソフトウェア実行シミュレーションによって，従来の MAC 手法と提案手法の実行コストの比較を行った．その結果， 提案手法は，デバイス認証の実行時間を約 1/8 倍に短縮，消費エネルギーを約 1/2 倍に低減可能であることを示した．

また，共同で研究を進めた学生が以下の表彰を受けた．

- Outstanding B4 Student Award, 1st. cross-disciplinary Workshop on Computing Systems, Infrastructures, and Programming

- Outstanding M1 Student Award, 1st. cross-disciplinary Workshop on Computing Systems, Infrastructures, and Programming

- コンピュータシステム研究会優秀若手デモ/ポスター賞，LSI とシステムのワークショップ 2017

- 2017 Excellent Student Award of The IEEE Fukuoka Section, IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing

５．主な発表論文等

- Mihiro Sonoyama, Takatsugu Ono, Haruichi Kanaya, Osamu Muta, Smruti R. Sarangi, Koji Inoue, “Radio Propagation Characteristics-based Spoofing Attack Prevention on Wireless Connected Devices,” IPSJ Transaction on Advanced Computer Systems, Feb. 2019.

- Mihiro Sonoyama, Takatsugu Ono, Haruichi Kanaya, Osamu Muta, Koji Inoue, “Wireless Spoofing-Attack Prevention Using Radio-Propagation Characteristics,” IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, Nov. 2017.

〔雑誌論文〕（計　1　件）

〔学会発表〕（計　5　件）

〔図書〕（計　0　件）

〔産業財産権〕
○出願状況（計　0　件）

○取得状況（計　0　件）

〔その他〕
ホームページ等

６．研究組織

(1)研究分担者
研究分担者氏名：なし