様式Ｆ－１９

# 科学研究費助成事業（学術研究助成基金助成金）研究成果報告書

平成　25 年　6 月　3 日現在

機関番号：12601
研究種目：挑戦的萌芽研究
研究期間：2011～2012
課題番号：23651164
研究課題名（和文）　衛星測位を利用した位置認証方法の開発

研究課題名（英文）　Position Authentication with Satellite-based Positioning

研究代表者　柴崎　亮介
（SHIBASAKI RYOSUKE）
東京大学　空間情報科学研究センター　教授
研究者番号：70206126

研究成果の概要（和文）：
GPS に加え多数の測位衛星システムが 2020 年までにサービスを開始する。位置情報の重要性は一層重要になる。たとえば、自動車の走行ルートに従って課金することができれば、柔軟な料金政策が可能になるだけでなく、料金所などの建設費用、混雑費用などを削減できる。しかしながら、位置情報の重要性が向上するにつれ、偽の位置情報を利用して課金を免れるなどの「位置騙し」が行われる可能性がある。そこで認証された位置情報を既存のインフラの大幅な改良や新規開発なしに生成する方法を開発した。具体的には、我々は GPS(QZSS)信号のリザーブビットに認証レファランス信号(RAND:Referance Authentication Navigation Data)を新規に定義して挿入、送信することで、それを受信して測位を行うケースには、真正な位置であることを証明できる。これは現行の GPS の信号構成に影響を及ぼさない。それをシミュレータを利用して実証した。なお衛星を利用して実証実験は地上からの信号送出のための地上局システム改良が間に合わず、実現できなかった。

研究成果の概要（英文）：
Many of GNSS or Global Navigation Satellite Systems in addition to GPS will start services until 2020. It enhances the importance of position information for society and industries. For example, GNSS will make it possible for us to collect tolls based on routes of individual vehicles. It is a very flexible toll or taxation system that can reduce the construction cost of or traffic congestion cost cause by toll gates. On the other hands, as position information become more critical, we may be threatened by “position-cheating” by sending fake position information to escape from toll collection or taxation. We developed a method of authenticating position information from GNSS without making large modification of the existing GNSS infrastructure or a new development. The method is to send newly defined “RAND:Referance Authentication Navigation Data” via QZSS (Quasi-Zenith Satellite System) and to enable users to authenticate position data created by receiving QZSS signal including RAND. This does not affect existing GNSS or GPS services and is easy to implement. We successfully tested an experimental system processing signals created with GNSS simulators. However, we could not conduct demonstration using real satellites due to the delay and cost of modification of the QZSS ground station.

交付決定額

（金額単位：円）

| | 直接経費 | 間接経費 | 合　計 |
|---|---|---|---|
| 交付決定額 | 3,100,000 | 930,000 | 4,030,000 |

研究分野：複合新領域
科研費の分科・細目：社会・安全システム科学・社会システム工学・安全システム

キーワード：ＧＰＳ信号、成りすまし、信号の脆弱性、認証信号

１．研究開始当初の背景

民生用ＧＰＳ信号は仕様書が公に公開されているので、GPS に似た信号を生成することも可能である。それゆえ、地上で誤った GPS 信号を送信することによって実際の GPS 信号を騙すことも可能である。これがいわゆるスプーフィング成りすましである。衛星からの到達信号を記憶して他の場所／時刻に向けて再送信することも可能である。これがいわゆるミーコニングである。その両者とも目的は、オリジナルの GPS 位置情報を変えることであり「位置情報ジャック」である。2008 年の ION 予稿集で T.E.Humphreys 氏らは簡易型 GPS 成りすまし受信機を使用し、スプーフィングの脅威を実証した。２００１年米国運輸省から発行された Volpe 報告書にこれらの問題は取り上げられていた。2012 のＩＯＮ(Institution of Navigation)でこの問題に関して話題性のある提案が多数(約 20 件弱)報告された。その提案の多くは、これから衛星を打ち上げて新規の開発するものであって、Galileo のように、信号構造の中に Anchi-Spoofing 技術を搭載する提案が報告された。一方で GPS 信号は実用化され送信されているので、現行の信号に新たな認証アルゴリズムを適用するような信号構造に変更することは不可能である。不幸なことに、新規に設計された民生用信号においてすらスプーフィングやミーコニングに対するいかなる防護策も持ち合わせていない。このため我々は QZSS 信号を使った GPS の認証アルゴリズムを開発するにいたった理由である。GPS を対象にしたのは位置とナビゲーションの信号でもっとも広く普及しているからである。本研究では位置とナビゲーションといった目的とするアプリケーションを超えて QZSS 衛星システムの唯一無比なアプリケーションを提案する。

２．研究の目的

本研究提案の目的は次の項目を達成することである。

（１）プロトタイプの認証受信機を開発する：GPS と QZSS の信号を演算できて認証データを分析することの可能な GNSS 受信機

（２）プロトタイプの認証データベースを開発する：秘匿された SEED 値、H-Matrix、公開鍵秘密鍵の割り当てをするのに不可欠な認証データベース

（３）衛星からの実際の生の GPS と QZSS 信号を使って認証全体システムを提示する：生データのデモは GPS と QZSS の衛星信号を使った認証アルゴリズムの有用性を証明できる。QZSS L1SAIF 信号がデモに使われる。

（４）現時点までの範囲でアルゴリズムを改善する：アルゴリズムは QZSS のＭＳ(Monitoring Station),MCS(Master Control Station)間のデータ遅延とデータ

アップデート遅延を分析することでさらに改善させる。

３．研究の方法

本方法はパリティビットを計算するユニークなアプローチであり、信号(A)（例えばGPS）の特定のナビゲーションデータを選び誤り訂正符合計算である LDPC(Low Density Parity Correction)エンコーデングを適用することである。その LDPC エンコーディングされたパリティビットをQZSS のような GPS と異なる衛星信号のナビゲーションメッセージのリザーブエリアに埋め込んで送信する。LDPC エンコーディングに不可欠な H-マトリクスは秘匿されて時間間隔に応じて変化する。

ナビゲーションメッセージに暗号をかけなければ、あるがままの信号には認証は必要でなく現行の受信機と同じで足りる。認証を必要としているユーザだけが、どこか遠方にあるデータサーバから秘密の鍵を受け取ってパリティビットをチェックする必要がある。このアプローチには次の 3 つの利点がある。

（1）受信機のハードウェアに改造を加えない

（2）現行の信号構成を利用できる

（3）異なるタイプの信号に適用できる QZSS,Galileo,Compass,L1SAIF,MSAS,EGNOS,GAGAN)

本方法は　民生用 GPS 信号と QZSS 信号を使って認証システムを設計することである。

QZSS は日本発のナビゲーション衛星システムである。測位衛星システムから位置とナビゲーションと時刻(PNT)のデータを提供する。しかしながら、PNT を超えたその他のデータを使ったサービスも可能である。『認証』とは民生信号を使った QZSS のサービスのひとつである。現在運行されている GPS，GLONASS の民生用信号はそのような能力が備わっていない。この点に関して日本が『認証』の能力ある QZSS を利用した宇宙技術の優位性を示すことは大変意義あり、重要である。

４．研究成果

プロトタイプ認証受信機は Superstar-II GPS 受信機のファームウェアを修正して開発された。そのファームウェアのプログラムは修正されて地上のコントロールセンタでＬ1SAIF 信号構造に適用できるので、L1SAIF メッセージに埋め込まれた認証データは QZSS 衛星にアップロード可能である。GPS と QZSS 衛星信号と認証受信機と認証データベースセンタをつかったテストとデモンストレーションを行った。数タイプの認証データ構造を定義してそれらのタイプごとの強み弱みを分析した。受信機と認証データベースセンタとの間での通信手段とセキュリティキーのやり取りも開発し、RSA のアルゴリズムに準拠して分析した。

**平成 23 年度**

プロトタイプ認証受信機 Superstar-II GPS 受信機のファームウェアを修正して開発された。受信機のファームウェアは GPS, QZSS(L1C/A,L1SAIF), MSAS, SBAS 信号を処理できるように変更した。受信機はさらに、認証データの処理も可能なように修正した。既存の GPS ボードでそのようにした理由は認証方法はファームウェアの修正だけで、いかなるハードウェアの変更も必要ないことをデモンストレーションするためである。

地上コントロールセンタでの L1SAIF 信号

の生成プログラムによってL1SAIFメッセージの中に認証データを適用できる。第一のデモは信号シミュレータを使って全体システムの機能の運用性をチェックすることである。ひとたび個々の構成要素の機能運用性がＯＫであればデモは次に GPS と QZSS の衛星信号を使って行う。この段階では、仮想の認証データベースセンタを使う。このデモではQZSS コントロールセンターにアクセスする必要があるので、我々は既にJAXAとの共同研究を締結してアルゴリズムの開発を行った。この共同研究は現在でも継続中である。同様の研究契約はENRIとSPACともL1SAIF信号について将来締結されると期待される。

平成 24 年度

プロトタイプ認証データベースセンター機能をPKI(公開鍵構成)の機能を包含して開発した。PKI は RSA アルゴリズムに基づき公開鍵、秘密鍵を使う。認証システムのコア部分であるセキュリティキーの管理を詳細に分析する必要がある。この段階で認証システムの全部のコンポーネントの準備ができて､GPS と QZSS からの生の衛星信号を使って実験ができる。地上局の信号送信システムを修正する作業がコストと費用の面から 24 年度注には行うことができなかったため、実衛星を利用したデモンストレーションは完了できなかったが、GNSS シミュレータにより技術的な検証は終了し、計画通りの効果があることが示された。

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 0 件）

〔学会発表〕（計 1 件）
第 6 回国際会議 (ICG;International Committee on Global Navigation Satellite System),2011 年 9 月、Dinesh Manandher

〔図書〕（計 0 件）

〔産業財産権〕
○出願状況（計 2 件）

名称：秘匿化された暗号ｺｰﾄﾞを用いた位置情報認証方法および位置情報認証システム
発明者：千野孝一、柴崎亮介、Dinesh Manandher
権利者：東大 TLO,㈱日立情報制御ソリューションズ
種類：特許
番号：特願 2009-187058
出願年月日：2009 年 8 月 12 日
国内外の別：国内

名称：位置情報認証方法および位置情報認証システム
発明者：千野孝一、柴崎亮介、Dinesh Manandher
権利者：東大 TLO,㈱日立情報制御ソリューションズ
種類：特許
番号：特願 2012-27791
出願年月日：2012 年 12 月 20 日
国内外の別：国内

○取得状況（計 1 件）

〔その他〕
ホームページ等

６．研究組織
(1)研究代表者
柴崎　亮介（SHIBASAKI RYOSUKE）
東京大学・空間情報科学研究センター・教授
研究者番号：70206126

(2)研究分担者
（　　）

研究者番号：

(3)連携研究者
（　　）

研究者番号：