Baseline Spoofing Detection for Aircraft with Standard Navigation Hardware

Michael Blois, John Studenny, Kyle O'Keefe, Baoyu Liu

Abstract: The spoofing detection technique presented uses the known baseline separation between GNSS antennas as the truth reference and compares it to calculated antenna baseline separation. The technique is based on the fact that the observed satellite time delay (phase information) is different at each antenna whereas a single antenna spoofer will provide exactly the same phase information at each antenna but slightly time delayed. When satellite data is used, the calculated antenna separation is a close match to the known baseline separation; when spoofer data is used, the calculated antennas separation collapses to zero. This technique is based on a known antenna separation and this known separation allows the computation of thresholds for false spoofing and missed spoofing. The consequence is that spoofing detection performance can be reliably quantified. Further, the desired spoofing performance will in-turn specify the minimum antenna baseline separation. The antenna separation can be calculated using either the pseudorange for a code phase solution or the carrier phase for RealTime-Kinematic (RTK) solution. Any off-the-shelf receiver-antenna can be used provided that it produces the data that enables the computation of a baseline solution. For the same spoofing detection performance, RTK allows for much shorter antenna baselines than a code phase solution. This spoofing detection technique does not require any specialized hardware, a pair off-the-shelf receiver-antenna is adequate. The experiment used a pair of NovAtel receiver-antennas with an off-the-shelf RTK software. The RTK software did not edit, screen or select "the most favorable data", all data were used from every sample instant as it were used in-flight. The spoofer was a GNSS signal repeater; however, this technique applies equally to a highly sophisticated spoofer. A truck was used to simulate an aircraft. The baseline solution separation (no spoofing) and baseline collapse (spoofing) performance correlates with theory.

Published in: Proceedings of the 36th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2023)
September 11 - 15, 2023
Hyatt Regency Denver
Denver, Colorado

Pages: 824 - 835

Cite this article: Blois, Michael, Studenny, John, O'Keefe, Kyle, Liu, Baoyu, "Baseline Spoofing Detection for Aircraft with Standard Navigation Hardware," *Proceedings of the 36th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2023)*, Denver, Colorado, September 2023, pp. 824-835.
https://doi.org/10.33012/2023.19413

標準的なナビゲーション・ハードウェアを搭載した航空機向けベースライン・スプーフィングの検出方法

マイケル・ブロワ、ジョン・スタデニー、カイル・オキーフ、バオユー・リウ

概要:
スプーフィング検出技術は、GNSS アンテナ間の既知の基線分離を真の基準として使用し、計算されたアンテナ基線分離と比較する。この技術は、観測された衛星の時間遅延(位相情報)が各アンテナで異なるという事実に基づいています。一方、単一アンテナのスプーファーは、各アンテナで全く同じ位相情報を提供しますが、わずかに時間遅延します。衛星データが使用される場合、計算されたアンテナセパレーションは既知のベースラインセパレーションとほぼ一致しますが、スプーファーデータが使用される場合、計算されたアンテナセパレーションは崩壊する結果、ゼロ値になってしまいます。この技術は既知のアンテナ分離に基づいており、この既知の分離により、偽のスプーフィングと見逃されたスプーフィングの閾値を計算することができます。その結果、スプーフィング検出性能を確実に定量化することができます。さらに、希望するスプーフィング性能は、最小アンテナ基線分離を特定します。アンテナ基線間隔は、コード位相ソリューションの場合は擬似距離、リアルタイムキネマティック(RTK)ソリューションの場合は搬送波位相を使って計算することができます。基線解の計算を可能にするデータを生成するものであれば、市販の受信アンテナを使用することができます。同じスプーフィング検出性能であれば、RTK はコード位相ソリューションよりもはるかに短いアンテナベースラインを可能にします。このスプーフィング検出技術には特別なハードウェアは必要なく、市販の受信機とアンテナのペアで十分です。実験では、市販の RTK ソフトウェアと NovAtel 社製受信アンテナのペアを使用した。RTK ソフトウェアは、編集、スクリーン、「最も好ましいデータ」の選択は行わず、すべてのサンプル・インスタントから、飛行中に使用されたデータをそのまま使用した。スプーファーは GNSS 信号の中継器であったが、この手法は高度に洗練されたスプーファーにも同様に適用できます。航空機の航跡を使用。ベースライン解分離(スプーフィングなし)とベースライン崩壊(スプーフィング)の性能は理論と相関した結果が得られました。

掲載誌:Proceedings of the 36th International Technical Meeting of the Institute of Navigation Satellite Division (ION GNSS+ 2023) September 11 - 15, 2023 Hyatt Regency Denver, Colorado

GNSS Spoofing Identification with Assistance of LEO Satellite Signal

Yiwei Wang, Yanhong Kou, and Zhigang Huang

Peer Reviewed

Abstract: To eliminate the impact of the spoofing signal on a GNSS receiver, it is necessary to correctly identify the spoofing signal from the authentic signal. However, this is difficult as the two signals take after each other with almost the same characteristics. To improve the spoofing identification capability of the receiver, we propose a two-stage anti-spoofing processing method: The parameters of the two signals are estimated by maximum-likelihood estimation (MLE) at the base-band signal processing level, and the corresponding pseudo-ranges are grouped according to their relative amplitude relationship or/and code-carrier Doppler frequency coherence (CCDC) relationship. The grouping result is then confirmed or corrected by calculating the residual of the least-square estimation (including the pseudo-range residuals or carrier Doppler residuals) of the navigation solution derived from each group of signal components. If the grouping result is proven to be self-consistent, the group of the spoofing signals is identified using the residual of the LSE integrating pseudo-ranges from 1 or 2 low earth orbits (LEO)that are not attacked by the spoofer. Otherwise, regrouping is performed by trial-and-error method until the residuals are small enough. Once spoofing signals are identified after incorporating the LEO pseudo-ranges, the tracking loops are forced to lock on the authentic sides. The performance of the proposed method is tested by simulation, and the results verify the effectiveness of the proposed method for anti-spoofing signal processing. The receiver can keep reporting correct position, velocity, and timing (PVT) information in the case of success, complete failure, and partial failure of spoofing pull-off.

Published in: Proceedings of the 2023 International Technical Meeting of The Institute of Navigation
January 24 - 26, 2023
Hyatt Regency Long Beach
Long Beach, California

Pages: 708 - 724

Cite this article: Wang, Yiwei, Kou, Yanhong, Huang, Zhigang, "GNSS Spoofing Identification with Assistance of LEO Satellite Signal," *Proceedings of the 2023 International Technical Meeting of The Institute of Navigation*, Long Beach, California, January 2023, pp. 708-724.
https://doi.org/10.33012/2023.18664

LEO 衛星信号の支援（アシスタント）による GNSS スプーフィング識別について

イウェイ・ワン、ヤンホン・コウ、ジガン・ファン

概要：
GNSS 受信機に対するスプーフィング信号の影響を排除するためには、スプーフィング信号と真正信号を正しく識別する必要がある。しかし、2 つの信号はほぼ同じ特性を持つため、この識別は困難である。受信機のなりすまし識別能力を向上させるために、我々は 2 段階のなりすまし防止処理方法を提案する：2 つの信号のパラメータをベースバンド信号処理レベルで最尤推定（MLE）し、対応する擬似レンジを相対的な振幅関係または/および符号搬送波ドップラー周波数コヒーレンス（CCDC）関係に従ってグループ化する。グループ化の結果は、各グループの信号成分から得られる航法解の最小二乗推定の残差（擬似レンジ残差または搬送波ドップラー残差を含む）を計算することによって確認または修正されます。グルーピング結果が自己整合的であることが証明された場合、スプーファーによって攻撃されていない 1 つまたは 2 つの低軌道（LEO）からの擬似レンジを積分した LSE の残差を使用して、スプーフィング信号のグループが識別されます。それ以外の場合は、残差が十分に小さくなるまで試行錯誤的に再グループ化を行う。LEO 擬似レンジを組み込んだ後、スプーフィング信号が特定されると、追跡ループは本物側にロックさせられます。提案手法の性能はシミュレーションによりテストされ、その結果、スプーフィング信号処理に対する提案手法の有効性が確認されました。受信機は、スプーフィングが成功した場合、完全に失敗した場合、部分的に失敗した場合においても、正しい位置、速度、タイミング（PVT）情報を報告し続けることができることになります。

掲載：Proceedings of the 2023 International Technical Meeting of The Institute of Navigation 2023 年 1 月 24 日～26 日 ハイアットリージェンシーロングビーチ カリフォルニア州ロングビーチ

GNSS Spoofing Mitigation Using Multiple Receivers

Niklas Stenberg, Erik Axell , Jouni Rantakokko, Gustaf Hendeby

Peer Reviewed

Abstract: GNSS receivers are vulnerable to spoofing attacks, where false satellite signals are transmitted to trick the receiver to provide false position and/or time estimates. Novel algorithms are proposed for spoofing mitigation by exchanging double differences of pseudorange, or carrier phase, measurements between multiple GNSS receivers. In scenarios where the spoofing system utilizes a single transmit antenna, the pseudorange, and carrier phase, measurements that are associated with the spoofing signal can be detected and removed. Simulated meaconing attacks generated with a Spirent hardware simulator and measurements obtained with a modified version of GNSS-SDR are used to evaluate the proposed algorithms. Spoofing mitigation using pseudorange measurements is possible, for receivers that are separated at least five meters apart. With a receiver separation of 20 meters, the pseudorange double difference algorithm is able to correctly authenticate at least six of seven pseudoranges within 30 seconds. The carrier phase approach enables mitigation of spoofing signals at shorter receiver distances. However, this approach requires a more accurate time synchronization between the receivers.

Published in: 2020 IEEE/ION Position, Location and Navigation Symposium (PLANS)
April 20 - 23, 2020
Hilton Portland Downtown
Portland, Oregon

Pages: 555 - 565

Cite this article: Stenberg, Niklas, Axell, Erik, Rantakokko, Jouni, Hendeby, Gustaf, "GNSS Spoofing Mitigation Using Multiple Receivers," *2020 IEEE/ION Position, Location and Navigation Symposium (PLANS)*, Portland, Oregon, April 2020, pp. 555-565.

複数受信機による GNSS スプーフィング緩和

ニクラス・ステンバーグ、エリック・アクセル、ヨウニ・ランタコッコ、グスタフ・ヘンデビー

概要:
GNSS 受信機は、偽の衛星信号を送信して受信機を欺き、偽の位置や時刻を推定させるスプーフィング攻撃に対して脆弱です。複数の GNSS 受信機間で擬似距離（搬送波位相）測定の二重差分を交換することで、スプーフィングを軽減する新しいアルゴリズムが提案されています。スプーフィングシステムが単一の送信アンテナを利用するシナリオでは、スプーフィング信号に関連する擬似距離と搬送波位相の測定値を検出し、除去することができます。提案アルゴリズムの評価には、Spirent ハードウェアシミュレータで生成されたミーコニング攻撃のシミュレーションと、GNSS-SDR の修正バージョンで得られた測定値が使用されています。少なくとも 5 メートル離れた受信機であれば、擬似距離測定を使用したスプーフィングの軽減が可能です。受信機の距離が 20 メートルの場合、擬似距離二重差分アルゴリズムは、30 秒以内に 7 つの擬似距離のうち少なくとも 6 つを正しく認証することができます。搬送波位相アプローチは、より短い受信距離でスプーフィング信号の軽減を可能にする。ただし、このアプローチでは、受信機間でより正確な時間同期が必要です。

掲載: 2020 IEEE/ION Position, Location and Navigation Symposium (PLANS) 2020 年 4 月 20 日～23 日 ヒルトン・ポートランド・ダウンタウン ポートランド オレゴン州

Intelligent Antennas for Mitigating GNSS Jamming & Spoofing Hazards on the ERTMS Train Control

Cosimo Stallo, Pietro Salvatori, Andrea Coluccia, Massimo Capozzi, Giovanni Gamba, Ernestina Cianca, Tommaso Rossi, Simone Di Domenico, Alessandro Neri, Francesco Rispoli, Massimiliano Ciaffi

Peer Reviewed

Abstract: The European Railways Train Management System (ERTMS) - the standard train control system largely adopted in the world to ensuring the highest safety levels - foresees the adoption of GNSS localization having been recognized as one of the Game Changer technologies to improve its competitiveness. The benefits of GNSS localization are in the savings of trackside balises that today ensures the periodical calibration of the errors accumulated by the odometer. However, the challenge is to guarantee that a virtual balise generated using the GNSS will be enough resilient to Radio Frequency threats, namely intentional or unintentional jamming. Since these threats can significantly degrade the GNSS localization performance up to a denial of service influencing the train operations, a proper mitigation strategy has been studied after having evaluated the operational scenarios of the ERTMS application. Currently, no commercial anti spoofing and anti-meaconing solution has been designed for the railway context. The solution we have developed is based on an intelligent antenna array to improve the resiliency of the PVT (Position, Velocity and Time) estimation performed by the VBR (Virtual Balise Reader) cleaning the signal from jamming, and to identify and exclude spoofing attacks. Since the antenna is the vulnerable gate of GNSS signals, a pre-evaluation of the RF (Radio Frequency) signals is performed before these signals are processed by the VBR. A comprehensive set of specific attacks, potentially harming the ERTMS under operational scenarios, has been investigated. These attackers – having been simulated either on board or along the rail corridor – are taken in to account to mitigate the blockage of the GNSS signal acquisition/tracking, and spoofers and meaconers potentially undermining the correct train positioning. The proposed paper will analyze and assess the risks of GNSS interferences on the ERTMS operational scenarios and will present a novel solution to mitigate these risks based on a four elements phased array antenna resulting a suitable compromise when cost and performance are considered. This approach is able to both detect and mitigate jamming generated along the rail corridor and to detect spoofing through its DoA (Direction of Arrival) estimation. The performance of this solution have been evaluated through extensive Montecarlo simulations to reproduce many complex different attack scenarios potentially occurring in the ERTMS operative conditions and to stress the system in order to fully reach the ERTMS SIL-4 requirement implying a Tolerable Hazards Rate (THR) of 10E-9h.

Published in: Proceedings of the ION 2019 Pacific PNT Meeting
April 8 - 11, 2019
Hilton Waikiki Beach
Honolulu, Hawaii

Pages: 478 - 492

Cite this article: Stallo, Cosimo, Salvatori, Pietro, Coluccia, Andrea, Capozzi, Massimo, Gamba, Giovanni, Cianca, Ernestina, Rossi, Tommaso, Di Domenico, Simone, Neri, Alessandro, Rispoli, Francesco, Ciaffi, Massimiliano, "Intelligent Antennas for Mitigating GNSS Jamming & Spoofing Hazards on the ERTMS Train Control," *Proceedings of the ION 2019 Pacific PNT Meeting*, Honolulu, Hawaii, April 2019, pp. 478-492.
https://doi.org/10.33012/2019.16818

欧州鉄道の列車管理システムにおける GNSS ジャミングとスプーフィングの危険性を軽減するインテリジェント・アンテナ

コジモ・スタッロ、ピエトロ・サルバトーリ、アンドレア・コルッチャ、マッシモ・カポッツィ、ジョヴァンニ・ガンバ、エルネスティーナ・チャンカ、トンマーゾ・ロッシ、シモーネ・ディ・ドメニコ、アレッサンドロ・ネーリ、フランチェスコ・リスポリ、マッシミリアーノ・チャフィ

概要：欧州鉄道列車管理システム（ERTMS）は、最高レベルの安全性を確保するために世界で広く採用されている標準的な列車制御システムですが、競争力を向上させるための Game Changer 技術の 1 つとして認識されている GNSS ローカライゼーションの採用を予見しています。GNSS ローカライゼーションの利点は、今日、走行距離計によって蓄積された誤差の定期的な校正を保証しているトラックサイド・バリス（Trackside balises（トラックサイド バリーゼ）”は、列車の自動運転や列車制御システムに関連する用語で、鉄道トラックの軌道沿いに設置された、無線通信やデータ伝送のための機器を指します。これは主に鉄道信号システムの一部として使用され、列車が位置情報を把握し、制御システムと通信するのに役立ちます。）の節約にあります。しかし、課題は、GNSS を使用して生成された仮想バリスが、意図的または非意図的な妨害電波という電波の脅威に対して十分な耐性を持つことを保証することです。これらの脅威は、列車の運行に影響を及ぼすサービス拒否に至るまで、GNSS 定位性能を著しく低下させる可能性があるため、ERTMS アプリケーションの運用シナリオを評価した後、適切な緩和戦略が研究されてきました。現在のところ、**商業的なアンチスプーフィングおよびアンチミーコニングソリューションは、鉄道コンテキスト用に設計されていません。**我々が開発したソリューションは、インテリジェント・アンテナ・アレイに基づいており、VBR（Virtual Balise Reader）によって実行される PVT（位置、速度、時間）推定の回復力を向上させ、妨害から信号をクリーニングし、スプーフィング攻撃を識別して排除します。アンテナは GNSS 信号の脆弱なゲートであるため、これらの信号が VBR によって処理される前に RF（無線周波数）信号の事前評価が実行されます。運用シナリオの下で ERTMS に害を及ぼす可能性のある特定の攻撃を包括的に調査しました。GNSS 信号の捕捉／追跡の妨害や、列車の正確な位置決めを損なう可能性のあるスプーファーやミーコナーを軽減するために、これらの攻撃者（車内または鉄道コリドー沿いでシミュレートされた）が考慮されている。提案する論文では、ERTMS の運用シナリオにおける GNSS 干渉のリスクを分析・評価し、コストと性能を考慮した場合に適切な妥協点をもたらす 4 素子フェーズドアレイアンテナに基づく、これらのリスクを軽減する新しいソリューションを提示する。このアプローチは、鉄道沿いで発生する妨害電波の検出と軽減、および DoA（到着方向）推定によるスプーフィングの検出の両方が可能である。このソリューションの性能は、大規模なモンテカルロ・シミュレーションによって評価され、ERTMS の運用条件下で発生する可能性のある複雑なさまざまな攻撃シナリオを再現し、許容危険率（THR）を意味する ERTMS SIL-4 要件に完全に到達するようにシステムにストレスを与えます。

掲載：Proceedings of ION 2019 Pacific PNT Meeting 2019 年 4 月 8 日～11 日 ヒルトン・ワイキキ・ビーチ（ハワイ州ホノルル

Jamming and Spoofing Impact on GNSS Signals for Railway Applications

Roman Ehrler, Andreas Wenz, Stefan Baumann, Paulo Mendes, Nikolas Dütsch, Alice Martin, Christian Hinterstocker

Peer Reviewed

Abstract: One target of the EGNSS MATE project is to analyze the influence of interferences such as jamming and spoofing on GNSS receivers and its impact on the safe localization of trains. As a basis, we use a data set collected over one year on an SBB measurement wagon traveling through the Swiss rail network using two different Global Navigation Satellite System receivers. A first analysis shows that receiver-based flags of jamming and spoofing events are overly sensitive and thus not useful for jamming and spoofing monitoring. Additionally, a heuristic decision algorithm is introduced using the correlation of the front-end gain and the carrier-to-noise power density. The results of the data analysis will be used to derive a set of testable requirements for future GNSS-based train localization solutions.

Published in: Proceedings of the 36th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2023)
September 11 - 15, 2023
Hyatt Regency Denver
Denver, Colorado

Pages: 4153 - 4167

Cite this article: Ehrler, Roman, Wenz, Andreas, Baumann, Stefan, Mendes, Paulo, Dütsch, Nikolas, Martin, Alice, Hinterstocker, Christian, "Jamming and Spoofing Impact on GNSS Signals for Railway Applications," *Proceedings of the 36th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2023)*, Denver, Colorado, September 2023, pp. 4153-4167.
https://doi.org/10.33012/2023.19384

ジャミングとスプーフィングが鉄道アプリケーションの GNSS 信号に与える影響

ローマン・エルラー、アンドレアス・ヴェンツ、シュテファン・バウマン、パウロ・メンデス、ニコラス・デュッチュ、アリス・マーティン、クリスティアン・ヒンターシュトッカー

査読付き

概要:
EGNSS MATE プロジェクトの目標の 1 つは、GNSS 受信機に対するジャミングやスプーフィングなどの干渉の影響と、列車の安全な定位への影響を分析することである。その基礎として、2 つの異なる全地球測位衛星システム受信機を使用してスイスの鉄道網を走行する SBB 測定ワゴンで 1 年間に収集されたデータセットを使用します。最初の分析により、受信機ベースの妨害・なりすまし事象のフラグは過敏であるため、妨害・なりすまし監視には役立たないことが示された。さらに、フロントエンド利得と搬送波対雑音電力密度の相関を利用した発見的判断アルゴリズムを導入する。データ解析の結果は、将来の GNSS ベースの列車定位ソリューションに対する一連のテスト可能な要件を導き出すために使用されます。

EGNSS MATE プロジェクトは、正確かつ安全な方法で列車の位置を特定するという問題に対するソリューションを開発することを目的としています。位置情報により、欧州交通管理システムでの移動ブロック操作が可能になり、既存の路線の容量増加と固定資産の削減が可能になります。このプロジェクトでは、地図支援センサー フュージョン アルゴリズムが DLR によって開発されます。アルゴリズムの開発には、スイスの通常軌間ネットワークのほとんどで必要なセンサー データを収集する SBB 車両を使用した測定キャンペーンが伴います。特定のシナリオをカバーするための追加の専用テストの実行が計画されています。IABG は、ERTMS 内での新しい Galileo サービス OSNMA および HAS の使用を分析し、ジャミングおよびスプーフィング攻撃に対するアルゴリズムのパフォーマンスをテストします。これはラボでシミュレートできます。このプロジェクトの結果は、開発されたアルゴリズムへのアクセスを提供し、将来の製品認証の基礎となるテスト カタログを作成することにより、ローカリゼーション ソリューションの標準化と信号業界内での製品開発の促進に役立ちます。
https://navisp.esa.int/project/details/221/show

掲載誌:Proceedings of the 36th International Technical Meeting of the Institute of Navigation Satellite Division (ION GNSS+ 2023) September 11 - 15, 2023 Hyatt Regency Denver Denver, Colorado

An Application for Detecting GNSS Jamming and Spoofing

Nicholas Spens, Dong-Kyeong Lee, Dennis Akos

Abstract: Global Navigation Satellite System (GNSS) location engines on Android devices provide incredible location and navigation utility to billions of people worldwide. However, these location engines currently have little to no protection from accidental or intentional tampering that could block service or even spoof the reported location. External sources of radio frequency interference (RFI) can jam or spoof GNSS signals, and a mock location can also be provided through software alone. The Android platform provides many native location metrics that can be used to detect and potentially mitigate these attacks. The GNSS Alarm Android application is being developed to test and implement various methods of spoofing/jamming detection. The application will be a standalone suite that provides multiple flags corresponding to each method with a target to provide to the public for testing and application pending further development. The app uses four different methods to detect attacks: comparing the GNSS and Network locations, checking the Android mock location flag, comparing the GNSS and System times, and observing the automatic gain control (AGC) and carrier to noise density (C/N0) signal metrics. The limitations of each testing method are explored, and potential improvements to the app are discussed.

Published in: Proceedings of the 34th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2021)
September 20 - 24, 2021
Union Station Hotel
St. Louis, Missouri

Pages: 1981 - 1988

Cite this article: Spens, Nicholas, Lee, Dong-Kyeong, Akos, Dennis, "An Application for Detecting GNSS Jamming and Spoofing," *Proceedings of the 34th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2021)*, St. Louis, Missouri, September 2021, pp. 1981-1988.
https://doi.org/10.33012/2021.18027

GNSS ジャミングとスプーフィングを検出するアプリケーション

ニコラス・スペンス、イ・ドンギョン、デニス・アコス

概要：
Android デバイスに搭載されている全地球衛星測位システム（GNSS）の位置情報エンジンは、世界中の何十億という人々に信じられないような位置情報とナビゲーションのユーティリティを提供している。しかし、これらの位置情報エンジンは現在、偶発的または意図的な改ざんからほとんど保護されておらず、サービスをブロックしたり、報告された位置を詐称したりする可能性があります。無線周波数干渉（RFI）の外部ソースは、GNSS 信号を妨害したり、なりすましたりする可能性があり、ソフトウェアだけで模擬位置を提供することもできます。Android プラットフォームは、これらの攻撃を検出し、潜在的に軽減するために使用することができる多くのネイティブの位置メトリックを提供します。GNSS アラーム Android アプリケーションは、スプーフィング/妨害検知の様々な方法をテストし実装するために開発されています。このアプリケーションは、各方法に対応する複数のフラグを提供する**スタンドアロンのアプリケーションです。**GNSS とネットワークの位置の比較、Android の模擬位置フラグのチェック、GNSS とシステムの時刻の比較、**自動利得制御（AGC）と搬送波対雑音密度（C/N0）の信号メトリクスの観察です。各テスト方法の限界について検討し、アプリの潜在的な改善点について議論します。**

掲載誌：ナビゲーション学会衛星部門第 34 回国際技術会議（ION GNSS+ 2021）議事録 2021 年 9 月 20 日～24 日 ユニオンステーションホテル セントルイス（ミズーリ州

Robust Dual -Antenna Receiver: Jamming/Spoofing Detection and Mitigation

Ali Broumandan, Thomas Taylor, Darrell Anklovitch, Sandy Kennedy

Abstract: GNSS receivers are highly vulnerable to structural interference signals such as spoofing and meaconing. A spoofing attack based on a set of synthesized GNSS signals, is an effective means of providing bogus position estimates to a victim receiver. Several spoofing countermeasure techniques to address different attack types using single or multiple antenna have been proposed. Both single and multiple antenna techniques focus on specific features of spoofing signals that can separate them from the authentic ones. Multiple antenna techniques can observe spoofing signals in ways that a single antenna cannot, and as a result they strengthen detection capabilities. Single antenna based spoofing detection metrics are implemented in the pre-despreading or post-despreading layers of a GNSS receiver and are most effective when both spoofing and authentic signals are present. Pre-despreading and intermediate frequency signal monitoring metrics have been used to detect the presence of excessive amount of power in GNSS bands. These metrics rely on the assumption that spoofing signals are more powerful than the authentic ones and that a successful spoofing attack transmits several GNSS-like signals. Post-despreading methods are used to detect an abnormal behavior in acquisition and tracking levels which is caused by the presence of both spoofing and authentic signals. In many practical scenarios, a spoofer generates multiple GNSS signals and transmits them using a single antenna. As such, spoofed PRNs are spatially correlated since they all experience the same propagation channel. This feature can be used to discriminate them from the spatially distributed authentic signals. More specifically, the counterfeit signals sourced from a single transmit antenna have the same spatial signature, which means that all the signals experience the same channel variation in the spatial domain. This can be used as a metric to detect a spoofing attack. A key advantage of multiple antenna over a single antenna spoofing detection is that it can detect a spoofing attack in the absence of authentic signals (e.g. covered antenna case). Additionally, when both authentic and spoofed signals are present, a multiple antenna based detection method can identify which particular PRNs are spoofed. This paper demonstrates a spoofing detection module implemented on a dual-antenna variant of NovAtel's OEM7 generation of GNSS receivers. The proposed architecture enables the receiver to detect a spoofing attack, as well as discriminate and classify spoofed PRNs from the authentic ones. The detector utilizes pre-despreading and post-despreading methods using a multi-layer detection strategy. The spatial processing detection metric uses two spatially separated antenna and is based on single and double-difference carrier phase observations. The operation of the proposed receiver structure will be tested in a real-world spoofing scenario. A hardware simulator is used as a spoofing generator, combined with the authentic signals collected from two spatially separated outdoor antennas. The test results show that the proposed technique can successfully detect and classify the spoofing and authentic PRNs. The advantage of a dual-antenna spoofing detection method will be compared to that of a single antenna in various spoofing attack scenarios. The detection performance of the dual-antenna spoofing detection methodology as a function of the antenna spacing will be characterized. The mean time to detect and probability of false detection in absence of spoofing attack will be evaluated in various GNSS operation environments.

Published in: Proceedings of the 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2020)
September 21 - 25, 2020

Pages: 1515 - 1532

Cite this article: Broumandan, Ali, Taylor, Thomas, Anklovitch, Darrell, Kennedy, Sandy, "Robust Dual -Antenna Receiver: Jamming/Spoofing Detection and Mitigation," *Proceedings of the 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2020)*, September 2020, pp. 1515-1532.
https://doi.org/10.33012/2020.17734

堅牢なデュアルアンテナ受信機：ジャミング/スプーフィングの検出と軽減

アリ・ブルマンダン、トーマス・テイラー、ダレル・アンクロビッチ、サンディ・ケネディ

概要：GNSS 受信機は、スプーフィングやミーコーニングのような構造的干渉信号に対して非常に脆弱である。合成された GNSS 信号のセットに基づくスプーフィング攻撃は、被害者の受信機に偽の位置推定を提供する効果的な手段です。単一アンテナまたは複数アンテナを使用する異なる攻撃タイプに対処するために、いくつかのスプーフィング対策技術が提案されています。シングルアンテナ技術もマルチアンテナ技術も、スプーフィング信号の特定の特徴に注目することで、本物の信号と区別することができます。マルチアンテナ技術は、シングルアンテナでは不可能な方法でスプーフィング信号を観測することができ、結果として検知能力を強化することができます。単一アンテナに基づくスプーフィング検出メトリクスは GNSS 受信機の前拡散または後拡散レイヤーに実装され、スプーフィング信号と真正信号の両方が存在する場合に最も効果的です。GNSS 帯域における過剰な電力の存在を検出するために、事前拡散と中間周波数信号モニタリング・メトリクスが使用されてきました。これらのメトリクスは、スプーフィング信号は真正信号よりも強力であり、成功したスプーフィング攻撃は複数の GNSS 類似信号を送信するという仮定に依存しています。ポスト拡散法は、スプーフィング信号と真正信号の両方が存在することによって引き起こされる捕捉レベルと追跡レベルの異常な動作を検出するために使用されます。多くの実用的なシナリオでは、スプーファーは複数の GNSS 信号を生成し、単一のアンテナを使って送信します。そのため、スプーフィングされた PRN はすべて同じ伝搬チャネルを経験するため、空間的に相関があります。この特徴を利用して、空間的に分散した本物の信号と識別することができます。より具体的には、1 つの送信アンテナから発信された偽造信号は同じ空間シグネチャを持ち、これは全ての信号が空間領域で同じチャネル変動を経験していることを意味する。これは、スプーフィング攻撃を検出するための手法として使用することができます。単一アンテナのスプーフィング検出に対する複数アンテナの主な利点は、本物の信号がない場合（例えばカバーアンテナの場合）でもスプーフィング攻撃を検出できることです。さらに、真正信号となりすまし信号の両方が存在する場合、マルチアンテナベースの検出方法は、どの特定の PRN がなりすましであるかを識別することができます。本論文では、NovAtel 社の OEM7 世代の GNSS 受信機のデュアルアンテナ型に実装されたスプーフィング検出モジュールを示します。提案するアーキテクチャにより、受信機はスプーフィング攻撃を検出し、スプーフィングされた PRN と本物の PRN を識別・分類することができます。この検出器では、マルチレイヤー検出ストラテジーを用いて、プリ拡散法とポスト拡散法を利用します。空間処理検出メトリックは、空間的に分離された 2 つのアンテナを使用し、単一および二重差分搬送波位相観測に基づいている。提案された受信機構造の動作は、実際のスプーフィングシナリオでテストされる。ハードウェアシミュレータがスプーフィングジェネレータとして使用され、空間的に分離された 2 つの屋外アンテナから収集された真正信号と組み合わされる。テスト結果は、提案技術がスプーフィングと真正 PRN の検出と分類に成功することを示している。様々なスプーフィング攻撃シナリオにおいて、デュアルアンテナによるスプーフィング検出方法の優位性をシングルアンテナによる検出方法と比較する。アンテナ間隔の関数としてのデュアルアンテナのスプーフィング検出方法の検出性能を特徴付ける。スプーフィング攻撃がない場合の平均検出時間と誤検出確率を様々な GNSS 運用環境で評価する。

掲載　　第 33 回国際航法学会衛星部門技術研究集会（ION GNSS+ 2020）予稿集
2020 年 9 月 21 日～25 日

A GNSS Jamming/Spoofing Test Suite for Smart Tachograph Applications

L. Cucchi, J. Fortuny, G. Baldini, I. Fernandez-Hernandez, B. Martinez, G. Vecchione

Abstract: It is well known that radio frequency interference (RFI) poses a threat to civil Global Navigation Satellite Systems (GNSS). This is particularly true in case of liability critical application in which the PVT information is directly related to legal and economic aspects. In the European Union (EU), the Smart Tachograph (ST), formerly known as Digital Tachograph, represents a typical example of liability-critical application in the road transportation domain. The ST is a good example of a regulated application in which GNSS plays a key role: the Position, Velocity and Timing (PVT) information is used by the Onboard Unit (OBU) in commercial vehicles above 3.5 tons (in goods transport) and carrying more than 9 persons including the driver (in passenger transport) in order to record the driving and resting time of drivers. In this context, PVT information is used by law enforcers to verify the compliance to the regulation ([Fig.1]). Hence, the risk of malicious actions aimed at tampering with the GNSS receiver or altering the PVT information, is high. A typology of the jamming and spoofing events in road applications has been defined, in order to create a test suite with the scenarios that are representative and of concern for the ST. The main goal of our activity is the development of a test suite aimed at supporting the adoption of the new EU Smart Tachograph regulatory framework; this means to support GNSS receiver manufacturers, ST manufacturers and ST integrators by sharing a reference test battery useful to assess the receiver robustness against jamming and spoofing within a harmonized context. The need to address the specific automotive scenario conditions and the requirements of the regulation has led to the development of an ad-hoc test suite. In particular, the test battery aims at simulating specific automotive dynamic and environment conditions with a wide range of jamming and spoofing events, including intentional and unintentional RFI events. In particular, 11 test cases have been developed and include three jamming, two repeaters and six spoofing scenarios: the RFI signals are superimposed on a baseline scenario, describing the ST trajectory and simulating nominal GPS and Galileo constellations. It is worth mentioning that the test battery fully supports the new Galileo OSNMA service as required by the regulation. Most of test cases last 20 minutes, while only one test case needs a longer simulation (i.e. 60 minutes). The same sampling frequency (i.e. 10 Msps) is used for all the test cases, while the bit depth varies from 8 to 16 bits depending on the presence of the jamming. The paper shows the laboratory set-up and the presents a detailed description of each test case. Moreover, some relevant results observed in the GNSS receivers under test are included even though this is not the main objective of the activity. The test campaign is still under preparation and in this phase, the main goal is to verify the proper design and implementation of the simulated scenarios. Once it is completed, the RFI sampled files and related detailed description will be shared among ST communities and any interested users.

Published in: Proceedings of the 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2020)
September 21 - 25, 2020

Pages: 1490 - 1514

Cite this article: Cucchi, L., Fortuny, J., Baldini, G., Fernandez-Hernandez, I., Martinez, B., Vecchione, G., "A GNSS Jamming/Spoofing Test Suite for Smart Tachograph Applications," *Proceedings of the 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2020)*, September 2020, pp. 1490-1514.
https://doi.org/10.33012/2020.17759

スマートタコグラフアプリケーションのための GNSS ジャミング/スプーフィング・テストに関する複数のアプリケーションセット（スイート）

L.クッキ、J.フォルチュニ、G.バルディーニ、I. フェルナンデス＝エルナンデス、B.マルティネス、G.ヴェッキオーネ

概要：無線周波干渉（RFI）が民間の全地球航法衛星システム（GNSS）に脅威を与えることはよく知られている。これは特に、PVT 情報が法的・経済的側面に直接関係するようなライアビリティー・クリティカルなアプリケーションの場合に当てはまります。欧州連合（EU）では、スマートタコグラフ（ST）（以前はデジタルタコグラフとして知られていた）が、道路交通領域におけるライアビリティクリティカルなアプリケーションの典型的な例です。ST は、GNSS が重要な役割を果たす規制アプリケーションの好例です。位置、速度、タイミング（PVT）情報は、3.5 トン以上の商用車（貨物輸送）および運転手を含む 9 人以上の乗客を乗せた商用車（旅客輸送）の車載ユニット（OBU）によって、運転手の運転時間と休憩時間を記録するために使用されます。このような背景から、PVT 情報は法執行官が規制遵守を確認するために利用される（[図 1]）。したがって、GNSS 受信機の改ざんや PVT 情報の改ざんを目的とした悪意のある行為のリスクは高い。ST が懸念する代表的なシナリオを含むテスト・スイートを作成するために、道路アプリケーションにおける妨害およびスプーフィング事象の類型が定義されています。これは、GNSS 受信機メーカー、ST メーカー、ST インテグレーターをサポートすることを意味し、妨害電波やなりすましに対する受信機のロバスト性を評価するために有用なリファレンステストバッテリーを、調和された状況で共有することを目的としています。特定の自動車シナリオの条件と規制の要件に対処する必要性から、アドホックテストスイートが開発されました。特に、このテスト・バッテリーは、意図的および非意図的な RFI イベントを含む、幅広い妨害およびスプーフィング・イベントを伴う特定の自動車の動的および環境条件をシミュレートすることを目的としている。特に、11 のテストケースが開発され、3 つの妨害、2 つのリピーター、6 つのスプーフィングシナリオが含まれています。テスト・バッテリーは、規制で要求されている新しい Galileo OSNMA サービスを完全にサポートしていることは特筆に値する。ほとんどのテストケースは 20 分ですが、1 つのテストケースだけがより長いシミュレーション（つまり 60 分）を必要とします。すべてのテストケースで同じサンプリング周波数（10Msps）が使用され、ビット深度は妨害電波の有無によって 8 ビットから 16 ビットに変化する。本論文では、実験室のセットアップを示し、各テストケースの詳細な説明を行う。さらに、この活動の主な目的ではないにもかかわらず、テスト中の GNSS 受信機で観測されたいくつかの関連する結果も含まれている。テストキャンペーンはまだ準備中であり、この段階での主な目標は、シミュレートされたシナリオの適切な設計と実装を検証することである。完了次第、RFI サンプリングファイルと関連する詳細な説明を ST コミュニティおよび関心のあるユーザー間で共有する予定です。

情報

スマートタコグラフ（Smart Tachograph）は、輸送業界で使用されるデジタル式のタコグラフ（運転記録装置）です。これは、トラックやバスなどの商業車両に搭載され、運転者の運転時間と休息時間を正確に記録するためのデバイスです。欧州連合（EU）では、ドライバーの労働時間や休息時間を管理する規制に基づき、車両にはタコグラフが必要です。

1. **位置情報の追跡:** GPS テクノロジーを使用して、車両の位置情報をリアルタイムで追跡します。これにより、運転時間や休息時間のコンプライアンスを詳細に管理できます。
2. **リアルタイム通信:** データ通信機能を備え、車両のデータを遠隔地の管理者にリアルタイムで送信できます。これにより、企業はドライバーの運転状況を把握しやすくなります。
3. **違反検知機能:** スマートタコグラフは、ドライバーが労働時間の規制に違反した場合や、違反のリスクが高まっている場合に警告を発する機能を備えています。
4. **運転者認証:** 個々のドライバーを識別し、正確な運転時間を各ドライバーに対して記録します。これにより、ドライバーごとの勤務時間を厳密に管理できます。
5. **データの保護:** スマートタコグラフは、データの安全性とセキュリティに重点を置いています。データの改竄を防ぐためにデジタル署名やセキュアな通信プロトコルが使用されます。

掲載　　第 33 回 ION GNSS+2020 国際衛星部門会議事録
2020 年 9 月 21 日～25 日

Development of Array Receivers with Anti-Jamming and Anti-Spoofing Capabilities with Help of Multi-Antenna GNSS Signal Simulators

Andriy Konovaltsev, Emilio Pérez Marcos, Manuel Cuntz, Michael Meurer, Ronald Wong, Guy Buesnel, Werner Lange

Abstract: The paper focuses on the use of GNSS constellation simulators for the performance evaluation of advanced anti-jamming and antispoofing techniques of GNSS receivers using multiple antennas in an antenna array. The use of antenna arrays and array signal processing enables a GNSS receiver to apply extremely efficient countermeasures to counteract radio frequency interference. This enhanced resilience to jamming and spoofing makes the multi-antenna GNSS receivers very attractive in the context of safety-critical applications. The paper highlights the advantages of testing such receivers in a controlled laboratory environment by utilizing the multi-antenna GNSS simulators. A fully scalable architecture of the multi-antenna simulator based on the use of multiple simulator units is presented. The simulator composed of 8 single RF output simulators is used together with a GNSS multi-antenna receiver prototype (GALANT) developed by DLR in order to obtain exemplary results for beamforming, direction of arrival estimation and spoofing detection in the corresponding signal scenarios. The obtained results are also used to highlight the merits of a GNSS array receiver as part of promising anti-jam and anti-spoof solutions.

Published in: Proceedings of the 32nd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2019)
September 16 - 20, 2019
Hyatt Regency Miami
Miami, Florida

Pages: 953 - 966

Cite this article: Konovaltsev, Andriy, Marcos, Emilio Pérez, Cuntz, Manuel, Meurer, Michael, Wong, Ronald, Buesnel, Guy, Lange, Werner, "Development of Array Receivers with Anti-Jamming and Anti-Spoofing Capabilities with Help of Multi-Antenna GNSS Signal Simulators," *Proceedings of the 32nd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2019)*, Miami, Florida, September 2019, pp. 953-966.
https://doi.org/10.33012/2019.16988

マルチアンテナ GNSS 信号シミュレータを用いたアンチジャミングおよびアンチスプーフィング機能を有するアレイ受信機の開発

アンドレイ・コノバルツェフ、エミリオ・ペレス・マルコス、マヌエル・カンツ、ミヒャエル・ミュラー、ロナルド・ウォン、ガイ・ビュースネル、ヴェルナー・ランゲ

概要：本論文では、アンテナアレイの複数のアンテナを使用する GNSS 受信機の高度なアンチジャミングおよびアンチスプーフィング技術の性能評価のための GNSS コンステレーションシミュレータの使用に焦点を当てている。アンテナアレイとアレイ信号処理を使用することで、GNSS 受信機は電波干渉に対抗するために非常に効率的な対策を適用することができます。このようにジャミングやスプーフィングに対する耐性が強化されたマルチアンテナ GNSS 受信機は、セーフティクリティカルなアプリケーションにおいて非常に魅力的なものとなっている。この論文では、マルチアンテナ GNSS シミュレータを利用することで、制御された実験室環境でこのような受信機をテストすることの利点を強調します。複数のシミュレータユニットを使用するマルチアンテナシミュレータの完全にスケーラブルなアーキテクチャを示す。DLR が開発した GNSS マルチアンテナ受信機プロトタイプ（GALANT）と共に、8 つの単一 RF 出力シミュレータで構成されるシミュレータを使用し、対応する信号シナリオにおけるビームフォーミング、到来方向推定、スプーフィング検出の模範的な結果を得る。また、得られた結果を用いて、GNSS アレイ受信機が有望なアンチジャムおよびアンチスプーフィングソリューションの一部であることを強調しています。

第 32 回 ION GNSS+2019 国際衛星部門技術会議講演論文集（Proceedings of the 32nd International Technical Meeting of the Institute of Navigation）
2019 年 9 月 16 日～20 日
ハイアット・リージェンシー・マイアミ
フロリダ州マイアミ

Analyzing the Impact of GNSS Spoofing on the Formation of Unmanned Vehicles Swarms

Aanjhan Ranganathan, Adam Belfki, Pau Closas

Abstract: In this paper, we explore the vulnerabilities and resilience of drone swarms to potential attacks, particularly focusing on the significance of accurate position information in the successful completion of swarm missions. We delve into the role of location spoofing attacks and assess the robustness of centralized versus distributed swarm communication architectures against such threats. Emphasizing the increasing adoption of distributed and decentralized algorithms, due to their adaptability and elimination of central control, our research centers on a scenario wherein a swarm aims for uniform distribution across a region, ensuring each drone covers equivalent areas. Such coverage tasks are vital for various applications, including surveillance and navigation. Using Voronoi tessellations and Lloyd relaxation, we identify possible attack vectors these missions might encounter. To assess the swarm behavior under location manipulations, we employ both a comprehensive framework integrating Gazebo, Ardupilot, and QGroundControl and a Python-based simulator. Our findings illuminate the challenges inherent to ensuring robust swarm operations and underscore avenues for future research aimed at bolstering swarm technology's defenses.

Published in: Proceedings of the 36th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2023)
September 11 - 15, 2023
Hyatt Regency Denver
Denver, Colorado

Pages: 3138 - 3147

Cite this article: Ranganathan, Aanjhan, Belfki, Adam, Closas, Pau, "Analyzing the Impact of GNSS Spoofing on the Formation of Unmanned Vehicles Swarms," *Proceedings of the 36th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2023)*, Denver, Colorado, September 2023, pp. 3138-3147.
https://doi.org/10.33012/2023.19438

無人機群形成における GNSS スプーフィングの影響の分析

アーンジャン・ランガナタン、アダム・ベルフキ、パウ・クロサス

概要：本論文では、群を構成するドローンの潜在的な攻撃に対する脆弱性と耐性を、特に群集ミッションの成功における正確な位置情報の重要性に焦点を当てながら探る。位置スプーフィング攻撃の役割を掘り下げ、このような脅威に対する集中型群通信アーキテクチャと分散型群通信アーキテクチャの堅牢性を評価する。その適応性と中央制御の排除により、分散・分散型アルゴリズムの採用が増加していることを強調し、我々の研究の中心は、群れが地域全体で均一な分布を目指し、各ドローンが同等のエリアをカバーすることを保証するシナリオである。このようなカバータスクは、監視やナビゲーションなど様々なアプリケーションに不可欠である。ボロノイテッセレーションとロイド緩和を用いて、これらのミッションが遭遇する可能性のある攻撃ベクトルを特定する。位置操作下での群動作を評価するために、Gazebo、Ardupilot、QGroundControl を統合した包括的なフレームワークと、Python ベースのシミュレータの両方を採用する。我々の発見は、堅牢な飛行群運用を確保するために固有の課題を明らかにし、飛行群技術の防御を強化することを目的とした今後の研究の道筋を強調するものである。

掲載　第 36 回 ION GNSS+2023 国際衛星部門会議事録
2023 年 9 月 11 日～15 日
ハイアット・リージェンシー・デンバー
コロラド州デンバー

Galileo Advanced Features for the Marine Domain: Breakthrough Applications for Safety and Security

Marie-Cécile Delmas, Kevin Salsac

Abstract: The GAMBAS project (Galileo Advanced features for the Maritime domain: Breakthrough Applications for Safety and security) is funded by the European Space Program Agency (EUSPA) under the European Union's Horizon 2020 research and innovation program under grant agreement no 101004292 aiming at identifying the Search-and-Rescue and Ship Security Alert System needs for maritime users (including operators and fishing stakeholders), and developing operational concepts to answer these needs. The general objective of the GAMBAS project is to support the deployment of Galileo exclusive features in the maritime domain, in order to improve: • safety and security at sea; • detection of illegal activities and associated surveillance means; • resilience to natural and human-induced emergency situations; and to develop, integrate, demonstrate, standardize and disseminate these new associated capabilities. The project aims to demonstrate: • improvement of the SAR (Search And Rescue) and SSAS (Ship Security Alert System) detection and response to maritime distress, through the integration of new features into the beacon for SSAS, in terms of cost optimization, user-friendly aspects, integration of Galileo and OS NMA (Open Service Navigation Message Authentication) reception for improved authenticated localization performance and reliability, and at sea triggering capabilities, • optimization of the responsiveness of RCCs (Rescue Coordination Center) towards the distress situations affecting vessels, • adaptation of the MCCs (Mission Control Center) and MEOLUT (Medium Earth Orbit Local User Terminal) to the data distribution of SSAS alerts.

Published in: Proceedings of the 35th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2022)
September 19 - 23, 2022
Hyatt Regency Denver
Denver, Colorado

Pages: 457 - 463

Cite this article: Delmas, Marie-Cécile, Salsac, Kevin, "Galileo Advanced Features for the Marine Domain: Breakthrough Applications for Safety and Security," *Proceedings of the 35th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2022)*, Denver, Colorado, September 2022, pp. 457-463.
https://doi.org/10.33012/2022.18490

海洋領域におけるガリレオの高度な機能：安全とセキュリティのための画期的なアプリケーション

マリー＝セシル・デルマス、ケビン・サルサック

概要：GAMBAS プロジェクト（Galileo Advanced features for the Maritime domain： Breakthrough Applications for Safety and security）は、欧州連合（EU）の Horizon 2020 研究・イノベーション・プログラムの下、欧州宇宙計画庁（EUSPA）により資金提供され、海上ユーザー（オペレーターや漁業関係者を含む）の捜索救助および船舶保安警報システムのニーズを特定し、これらのニーズに応える運用コンセプトを開発することを目的としている。GAMBAS プロジェクトの一般的な目的は、以下を改善するために、海上領域におけるガリレオ専用機能の展開を支援することである： - 海上における安全とセキュリティ、違法行為の検知と関連する監視手段、自然および人為的な緊急事態に対する回復力、これらの新しい関連能力の開発、統合、実証、標準化、普及。プロジェクトの目的は以下の通りである： - SAR（捜索救助）と SSAS（船舶保安警報システム）の検知と遭難への対応の改善。SSAS 用ビーコンに新機能を統合することにより、コストの最適化、ユーザー・フレンドリーな側面、ガリレオと OS NMA（オープン・サービス・ナビゲーション・メッセージ認証）の統合による認証されたローカライゼーションの性能と信頼性の向上、 船舶に影響を及ぼす遭難状況に対する RCC（救助調整センター）の応答性の最適化、MCC（ミッション・コントロール・センター）と MEOLUT（中軌道ローカル・ユーザー・ターミナル）の SSAS アラートのデータ配信への適応。

掲載　 第 35 回 ION GNSS+2022 国際衛星部門会議事録
2022 年 9 月 19 日～23 日
ハイアット・リージェンシー・デンバー
コロラド州デンバー

AI-based GNSS Spoofing Attack Detection for Autonomous Vehicles using Satellite Characteristics Data

Sagar Dasgupta, Mizanur Rahman, Thejesh N. Bandi

Abstract: Autonomous vehicles (AVs) will radically change the transportation landscape in the coming years. AVs' localization and navigation systems primarily depend on the global navigation satellite systems (GNSS). However, the lack of encryption and low signal strength make GNSS signals vulnerable to intentional and unintentional threats. Out of all intentional threats, spoofing is a sophisticated and detrimental type of attack in which an attacker can manipulate and override the original GNSS signal, and an AV's GNSS receiver receives false position and tracking information – misled by the spoofer. In this way, an AV can be incrementally directed to the wrong destination, compromising the user's safety and security. This paper presents a novel approach for detecting GNSS spoofing attacks where clock correction polynomial parameters, ephemeris parameters, and integrity data (CEI) from the visible satellites are used to detect a spoofing attack in real time. We hypothesize that the pattern of certain CEI time series variables could change during a spoofing attack. Therefore, understanding and learning the pattern of CEI variables will help identify anomalies in GNSS signals at any given instance. Our approach investigates a recurrent neural network, a Long Short Term Memory (LSTM) network, trained with authenticated GNSS signals over a duration to detect the anomaly in the variable values due to an attack. GNSS datasets may include satellite signal data from different satellite systems, such as GPS, Galileo, GLONASS, and BeiDou, which are used to train the AI model. The AI-based detection model is evaluated using the GNSS spoofing attack and attack-free datasets. The evaluation results prove the potential of our approach toward a robust solution.

Published in: Proceedings of the 2023 International Technical Meeting of The Institute of Navigation
January 24 - 26, 2023
Hyatt Regency Long Beach
Long Beach, California

Pages: 514 - 525

Cite this article: Dasgupta, Sagar, Rahman, Mizanur, Bandi, Thejesh N., "AI-based GNSS Spoofing Attack Detection for Autonomous Vehicles using Satellite Characteristics Data," *Proceedings of the 2023 International Technical Meeting of The Institute of Navigation*, Long Beach, California, January 2023, pp. 514-525. https://doi.org/10.33012/2023.18608

衛星特性データを用いた AI による自律走行車の GNSS スプーフィング攻撃検知

サガー・ダスグプタ、ミザヌール・ラーマン、テジェシュ・N・バンディ

概要：自律走行車（AV）は、今後数年間で交通の状況を根本的に変えるだろう。AV の定位とナビゲーションシステムは、主に全地球航法衛星システム（GNSS）に依存している。しかし、GNSS 信号は暗号化されておらず、信号強度も低いため、意図的・非意図的な脅威に対して脆弱である。意図的な脅威の中でも、スプーフィングは洗練された有害なタイプの攻撃で、攻撃者はオリジナルの GNSS 信号を操作して上書きすることができ、AV の GNSS レシーバーはスプーファーに惑わされた偽の位置と追跡情報を受信します。このようにして、AV は誤った目的地へ段階的に誘導され、ユーザーの安全性とセキュリティを損なう可能性があります。この論文では、GNSS スプーフィング攻撃を検出するための新しいアプローチを紹介します。このアプローチでは、クロック補正多項式パラメータ、エフェメリスパラメータ、および可視衛星からの完全性データ（CEI）を使用して、スプーフィング攻撃をリアルタイムで検出します。我々は、なりすまし攻撃中に、CEI の時系列変数のパターンが変化する可能性があると仮定している。したがって、CEI 変数のパターンを理解し学習することは、任意のインスタンスにおける GNSS 信号の異常を特定するのに役立つ。我々のアプローチでは、攻撃による変数値の異常を検出するために、認証された GNSS 信号で長期間にわたって訓練されたリカレントニューラルネットワーク、LSTM（Long Short Term Memory）ネットワークを調査する。GNSS データセットには、GPS、Galileo、GLONASS、BeiDou などの異なる衛星システムからの衛星信号データが含まれることがあり、これらは AI モデルの学習に使用されます。AI ベースの検出モデルは、GNSS スプーフィング攻撃と攻撃なしのデータセットを用いて評価されます。評価結果は、堅牢なソリューションに向けた我々のアプローチの可能性を証明している

掲載：Proceedings of the 2023 International Technical Meeting of The Institute of Navigation 2023 年 1 月 24 日～26 日 ハイアットリージェンシーロングビーチ カリフォルニア州ロングビーチ

Enhancements Enabled by Multi-Element Antennas for GPS Anti-jamming Capabilities in Civil Applications

Bradford W, Parkinson, Chris Bartone

Abstract: The US Position, Navigation and Time (PNT) Advisory Board has adopted a strategy of "PTA" to ensure PNT is available for all users. The acronym stands for Protection, Toughening, and Augmentation. Elaboration can be found at (Parkinson 2022). This paper will summarize the Toughening Strategy part of the PTA and the four major techniques that a GPS receiver system can use for this purpose: 1. Signal Processing; 2. Use of Inertial Components to narrow bandwidths and enable fly-wheeling of position; 3. Controlled Reception Pattern Antennas (CRPAs - particularly digital, multi- element antennas), and 4. Satellite Enhancements such as multiple constellations, additional signals/frequencies, and increased broadcast Effective Isotropic Radiated Power (EIRP). The focus of this paper is the 3rd technique, use of CRPAs. The utilizations of multi-element GPS CRPAs have been around since the early developments of GPS. (Henderson 1980) (Euler 1984) (Hudak 1986) The US government continues to restrict the use of these multi-element antennas as part of their Export Control/International Traffic in Arms Regulations (EC/ITAR). (Title 22 Part 121 US) The recent development of high-speed, inexpensive analog to digital converters is changing the cost and availability of this toughening technique. For example, the US restriction to no more than three antenna elements is not generally honored outside the US. Internationally, existing products and companies offer 8-element and 16-element antenna array products. (Tualcom 2023) These internationally available CRPAs are multi-frequency and multi-constellations (GPS, GLONASS, BeiDou, SBAS, QZSS) Thus, these US EC/ITAR restrictions are effectively eliminating US civil manufacturers from competing and offering commercial-based products for GNSS Anti-Jam (AJ) applications. More important, these restrictions are inhibiting the applications of the GNSS AJ CRPA technologies in critical applications, such as US civil aircraft, ships, autonomous and remotely piloted vehicle (RPV) platforms. Recent research at Ohio University has quantified the value of these antennas to a GPS receiver for differing numbers of antenna elements. (Bartone 2011) This quantification is usually measured as decibels of gain in the direction of the desired (D) GPS signal minus the attenuation of the null that such antennas can present in the direction of an undesired (U) jamming source. A major purpose of the paper is to quantify the value of multi-element antennas in reducing the effectiveness against an array of six 100 Watt jammers. Several CRPA configurations are considered to illustrate the operational effectiveness in reducing the effects of jamming interference for civil applications. For example, a 20 dB improvement in gain-to-null ratio (i.e., D/U) will reduce the jammer line-of-sight area by 99%, while reducing the radius of effectiveness by 90%. This paper discusses several aspects of the current EC/ITAR regulations. The techniques have been well known for over 50 years, and the constraints are not being honored elsewhere in the world. Thus, the paper will make the case for removing these, largely inhibiting, EC/ITAR restraints and unleashing the US manufacturer's creativity in greatly reducing the GPS jamming problem for critical civil applications.

Published in: Proceedings of the 36th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2023)
September 11 - 15, 2023
Hyatt Regency Denver
Denver, Colorado

民生用途における GPS 妨害防止機能のマルチエレメント アンテナによって実現される機能強化

ブラッドフォード・W、パーキンソン、クリス・バートン

概要：米国の位置・航法・時刻（PNT）諮問委員会は、PNT をすべてのユーザーが利用できるようにするため、「PTA」という戦略を採用した。この頭字語は、Protection（保護）、Toughening（強化）、Augmentation（補強）の頭文字をとったものである。詳しくは（Parkinson 2022）を参照されたい。この論文では、PTA の Toughening Strategy の部分と、GPS 受信機システムがこの目的のために使用できる 4 つの主要な技術について要約します：1.信号処理、2.帯域幅を狭め、位置のフライホイールを可能にするための慣性コンポーネントの使用、3.制御された受信パターンアンテナ（CRPA - 特にデジタル、マルチエレメントアンテナ）、および 4. 複数のコンステレーション、追加信号／周波数、放送有効等方性放射電力（EIRP）の増加などの衛星の強化。本論文の焦点は、3 番目の手法である CRPA の使用です。マルチエレメント GPS CRPA の利用は、GPS の開発初期からありました。（Henderson 1980）（Euler 1984）（Hudak 1986） 米国政府は、輸出規制/国際武器取引規制（EC/ITAR）の一環として、これらのマルチエレメン ト・アンテナの使用を制限し続けています。（最近、高速で安価なアナログ・デジタル変換器が開発され、この強化技術のコストと入手可能性が変化しつつある。例えば、アンテナエレメントは 3 つまでという米国の制限は、米国外では一般的に守られていません。国際的には、既存の製品や企業が 8 素子や 16 素子のアンテナアレイ製品を提供しています。（これらの国際的に利用可能な CRPA は多周波数、多コンステレーション（GPS、GLONASS、BeiDou、SBAS、QZSS）であるため、このような米国の EC/ITAR の制限は、米国の民間メーカーが GNSS アンチジャム（AJ）アプリケーションのために商業ベースの製品を競争し提供することを事実上排除している。さらに重要なことは、これらの規制が、米国の民間航空機、船舶、自律型および遠隔操縦車両（RPV）プラットフォームなどの重要なアプリケーションにおける GNSS AJ CRPA 技術のアプリケーションを阻害していることです。オハイオ大学の最近の研究では、アンテナ素子数が異なる場合の GPS 受信機に対するこれらのアンテナの価値が定量化されました（Bartone 2011）。（Bartone 2011） この数値化は通常、希望する（D）GPS 信号の方向における利得のデシベル数から、そのようなアンテナが望ましくない（U）妨害信号源の方向で示すことができるヌルの減衰を差し引いた値として測定されます。本論文の主な目的は、6 つの 100 ワット・ジャマーのアレイに対する効果を低減するマルチ・エレメント・アンテナの価値を定量化することである。民間アプリケーションにおける妨害電波の影響を低減する運用上の有効性を説明するために、いくつかの CRPA 構成が検討されている。例えば、利得対ヌル比（すなわち D/U）を 20dB 改善すると、有効半径を 90%減少させながら、ジャマーの見通し線エリアを 99%減少させることができる。本稿では、現行の EC/ITAR 規制のいくつかの側面について述べる。この技術は 50 年以上前からよく知られており、その制約は世界の他の場所では守られていない。このため、本稿では、EC/ITAR による制約を撤廃し、重要な民間アプリケーションにおける GPS 妨害問題を大幅に軽減するために、米国メーカーの創造性を解き放つことを主張します。

掲載　第 36 回 ION GNSS+2023 国際衛星部門会議事録
2023 年 9 月 11 日～15 日
ハイアット・リージェンシー・デンバー
コロラド州デンバー

Multi-Frequency, Multi-Constellation INS-Assisted GNSS for Improved Navigation Under Jamming Conditions

Abdelsatar Elmezayen, Haidy Elghamrawy, Malek Karaim, Aboelmagd Noureldin

Peer Reviewed

Abstract: The low power of global navigation satellite system (GNSS) signals and their vulnerability to disruption sources, such as signal jamming, can cause severe degradation or interruption in GNSS position, navigation, and timing services. However, the modernization of GPS with multi-frequency signals and the availability of signals from multi-constellation GNSS systems such as Galileo and GLONASS increase the immunity of GNSS-based navigation to signal jamming. Integration of GNSS and inertial navigation systems (INS) in one navigation system can also provide better performance than standalone systems. This paper aims to evaluate the performance of GNSS receivers under jamming conditions when accessing GPS only and when enabling Galileo and GLONASS signals. Experiments were performed using advanced GNSS signal simulators to generate semi-real data sets. The performance of a standalone GNSS receiver and the integrated GNSS/INS system was evaluated under different jamming power levels. Results have shown higher resistance to signal jamming when allowing access to multiple frequencies on GPS other than L1 only. Enabling signals from multiple GNSS constellations further improved the receiver's anti-jamming capabilities. Integration of the GNSS receiver's output with a navigation solution from INS increased the robustness of the system in terms of navigation under signal jamming conditions.

Published in: Proceedings of the 36th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2023)
September 11 - 15, 2023
Hyatt Regency Denver
Denver, Colorado

Pages: 3849 - 3860

Cite this article: Elmezayen, Abdelsatar, Elghamrawy, Haidy, Karaim, Malek, Noureldin, Aboelmagd, "Multi-Frequency, Multi-Constellation INS-Assisted GNSS for Improved Navigation Under Jamming Conditions," *Proceedings of the 36th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2023)*, Denver, Colorado, September 2023, pp. 3849-3860.
https://doi.org/10.33012/2023.19389

多周波数、マルチコンステレーションの INS 支援 GNSS により妨害電波状況下でのナビゲーション向上策

アブデルサタール・エルメザイエン、ハイディ・エルガムラウィ、マレク・カライム、アボエルマグド・ノウレルディン

概要：全地球航法衛星システム（GNSS）信号は低電力であり、信号妨害などの妨害源に対して脆弱であるため、GNSS の位置、航法、タイミングサービスに深刻な劣化や中断を引き起こす可能性があります。しかし、マルチ周波数信号による GPS の近代化と、Galileo や GLONASS のようなマルチコンステレーション GNSS システムからの信号の利用可能性により、信号妨害に対する GNSS ベースのナビゲーションの耐性が向上しています。また、GNSS と慣性航法システム（INS）を 1 つのナビゲーション・システムに統合することで、独立したシステムよりも優れた性能を提供することができます。本論文の目的は、GPS のみにアクセスする場合と、Galileo と GLONASS の信号を有効にする場合の、妨害条件下での GNSS 受信機の性能を評価することである。先進的な GNSS 信号シミュレータを使用して実験を行い、準実データセットを使用しています。スタンドアロン GNSS レシーバーと統合 GNSS/INS システムの性能が、異なる妨害電波パワーレベル下で評価されました。その結果、L1 以外の GPS の複数の周波数にアクセスできるようにした方が、信号妨害に対する耐性が高くなることが示されました。複数の GNSS コンステレーションからの信号を利用可能にすることで、受信機のアンチジャミング能力はさらに向上しました。GNSS 受信機の出力を慣性航法システムのナビゲーション・ソリューションと統合することで、信号妨害条件下でのナビゲーションという点で、システムの堅牢性が向上しました。

掲載　　第 36 回 ION GNSS+2023 国際衛星部門会議事録
2023 年 9 月 11 日～15 日
ハイアット・リージェンシー・デンバー
コロラド州デンバー

Discrete Mathematical Model for GNSS Interference Detection Using ADS-B Quality Parameters

Jakub Steiner, Ivan Nagy

Peer Reviewed

Abstract: The growing dependence of critical infrastructure on Global Navigation Satellite Systems (GNSS) as an accurate and reliable positioning, navigation and timing (PNT) source gives rise to the importance of GNSS interference detection. Although jamming detection capabilities are present in the current market, predominately in the form of specialised GNSS interference detectors or GNSS receivers add-ons. These provide a limited coverage area and their implementation into critical infrastructure operations is rather slow. Therefore, this paper focuses on the detection of GNSS interference using widespread Automatic Dependent Surveillance-Broadcast (ADS-B) technology. The research builds upon previous work and addresses some of its limitations by developing a discrete mathematical model for GNSS jamming detection based on ADS-B quality parameters. To develop and validate the model, a series of experiments involving GNSS jamming in live-sky environments were conducted. The controlled experiments enabled close monitoring of the aircraft navigation systems allowing for precise determination of the aircraft's jammed/unjammed status. Approximately 75% of the jamming experiment data was used for model development and tuning, while the remaining 25% was reserved for evaluation. The model evaluation leveraging the confusion matrix showed a positive jamming detection rate of over 99% and a false positive jamming detection rate of under 1%. Additionally, the model was tested on ADS-B data from the Atlantic Ocean where no GNSS jamming is expected. Using this data set the model exhibited an under 1% false positive jamming detection rate.

Published in: Proceedings of the 36th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2023)
September 11 - 15, 2023
Hyatt Regency Denver
Denver, Colorado

Pages: 4145 - 4152

Cite this article: Steiner, Jakub, Nagy, Ivan, "Discrete Mathematical Model for GNSS Interference Detection Using ADS-B Quality Parameters," *Proceedings of the 36th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2023)*, Denver, Colorado, September 2023, pp. 4145-4152.
https://doi.org/10.33012/2023.19383

ADS-B 品質パラメータを使用した GNSS 干渉検出用の離散数学モデル

ヤクブ・シュタイナー、イヴァン・ナジ

概要:
正確かつ信頼性の高い測位、ナビゲーション、タイミング（PNT）ソースとしての重要なインフラストラクチャの全地球航法衛星システム（GNSS）への依存度が高まっているため、GNSS 干渉検出の重要性が高まっています。現在の市場には妨害検出機能が存在しますが、主に専用の GNSS 干渉検出器または GNSS 受信機アドオンの形で使用されています。これらは提供できる範囲が限られており、重要なインフラストラクチャ運用への実装はかなり時間がかかります。したがって、この論文では、広く普及している自動従属監視ブロードキャスト（ADS-B）テクノロジーを使用した GNSS 干渉の検出に焦点を当てます。この研究は以前の研究に基づいて構築されており、ADS-B 品質パラメータに基づいた GNSS 妨害検出のための離散数学モデルを開発することで、その制限の一部に対処しています。モデルを開発して検証するために、ライブスカイ環境での GNSS 妨害を含む一連の実験が実施されました。制御された実験により、航空機のナビゲーション システムを綿密に監視することが可能になり、航空機のジャミング状態/非ジャミング状態を正確に判断できるようになりました。妨害実験データの約 75% はモデルの開発と調整に使用され、残りの 25% は評価用に確保されました。混同行列を活用したモデル評価では、99% を超える肯定的な妨害検出率と 1% 未満の誤検出妨害検出率が示されました。さらに、このモデルは、GNSS 妨害が予想されない大西洋からの ADS-B データでテストされました。このデータセットを使用すると、モデルは 1% 未満の誤検知妨害検出率を示しました。

補足説明:ADS-B（Automatic Dependent Surveillance-Broadcast）は、航空機の位置やその他の情報を自動的にブロードキャストする技術です。これは航空交通管理（ATM）や航空機の監視において使用されます。ADS-B は GPS データを基にしたもので、航空機が自身の位置情報を放送するためのシステムのこと。

第 36 回航法研究所衛星部門国際技術会議（ION GNSS+ 2023）の議事録 2023 年
9 月 11 ～ 15 日
ハイアット リージェンシー デンバー
コロラド州デンバー

Developing Test Scenarios for Assessing Receiver Capabilities & Vulnerabilities of GNSS Radio Frequency Interference Monitors

Sherman Lo, Yu Hsuan Chen, Nicolas San Miguel, Hagop Chinchinian, Todd Walter, Dennis Akos

Abstract: As man-made and deliberate threats to global navigation satellite systems (GNSS) grow, it becomes increasing important to have an ability to quickly detect, characterize and even possibly localize GNSS radio frequency interference (RFI). Developing GNSS monitors capable of accurately and quickly detecting RFI (jamming and spoofing) require a means of testing both the hardware capabilities and the algorithms being created. In our past work, we described and utilized a set up to test GNSS equipment under RFI (San Miguel, et al., 2022, 2023, Chen, et al., 2023). This paper builds on that work with the final goal to develop a baseline set of spoofing and interference test scenarios to span both common and challenging potential threats. This allows us to assess the capabilities of our receiver/monitor and develop suitable algorithms. This paper will discuss what is needed for the baseline set and how we can build the set. The needed scenarios will depend on the purpose of the GNSS receiver. Since we want the scenarios widely accessible, publicly available sets are used when available supplemented by scenarios generated by Stanford to cover gaps. This paper discusses how these scenarios may be generated and what should be provided to allow for proper evaluation. Finally, it will show some simple example scenarios that we are developing to illustrate the benefits and challenges of producing good scenarios.

Published in: Proceedings of the 36th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2023)
September 11 - 15, 2023
Hyatt Regency Denver
Denver, Colorado

Pages: 1259 - 1275

Cite this article: Lo, Sherman, Chen, Yu Hsuan, Miguel, Nicolas San, Chinchinian, Hagop, Walter, Todd, Akos, Dennis, "Developing Test Scenarios for Assessing Receiver Capabilities & Vulnerabilities of GNSS Radio Frequency Interference Monitors," *Proceedings of the 36th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2023)*, Denver, Colorado, September 2023, pp. 1259-1275.
https://doi.org/10.33012/2023.19454

GNSS 無線周波数干渉モニターの受信機機能と脆弱性を評価するためのテストシナリオの開発

シャーマン・ロー、ユー・シュアン・チェン、ニコラス・サン・ミゲル、ハゴップ・チンチニアン、トッド・ウォルター、デニス・エイコス

全地球測位衛星システム（GNSS）に対する人為的かつ意図的な脅威が増大するにつれて、GNSS 無線周波数干渉（RFI）を迅速に検出、特徴づけ、さらには位置特定する能力を持つことがますます重要になっています。RFI（ジャミングおよびスプーフィング）を正確かつ迅速に検出できる GNSS モニターを開発するには、ハードウェアの機能と作成されるアルゴリズムの両方をテストする手段が必要です。私たちの過去の研究では、RFI に基づいて GNSS 機器をテストするためのセットアップを説明し、利用しました（San Miguel, et al., 2022, 2023、Chen, et al., 2023）。このペーパーは、その作業に基づいて構築されており、一般的な潜在的脅威と困難な潜在的脅威の両方に及ぶスプーフィングと干渉のテスト シナリオのベースライン セットを開発するという最終目標を掲げています。これにより、受信機/モニターの機能を評価し、適切なアルゴリズムを開発することができます。このペーパーでは、ベースライン セットに必要なものと、そのセットを構築する方法について説明します。必要なシナリオは、GNSS 受信機の目的によって異なります。シナリオを広くアクセスできるようにするため、利用可能な場合は公開セットが使用され、ギャップを埋めるためにスタンフォード大学が生成したシナリオで補完されます。このペーパーでは、これらのシナリオがどのように生成されるか、および適切な評価を可能にするために何を提供する必要があるかについて説明します。最後に、優れたシナリオを作成する利点と課題を説明するために開発中のいくつかの簡単なシナリオ例を示します。

第 36 回航法研究所衛星部門国際技術会議 (ION GNSS+ 2023) の議事録 2023 年
9 月 11 ～ 15 日
ハイアット リージェンシー デンバー
コロラド州デンバー

これら記事を引用している: Lo、Sherman、Chen、Yu Hsuan、Miguel、Nicolas San、Chinchinian、Hagop、Walter、Todd、Akos、Dennis、「GNSS 無線周波数干渉モニターの受信機能力と脆弱性を評価するためのテスト シナリオの開発」、第 36 回国際技術会議議事録航法研究所衛星部門会議（ION GNSS+ 2023）、コロラド州デンバー、2023 年 9 月、1259 ～ 1275 ページ。
https://doi.org/10.33012/2023.19454

Characterization of LTE Jamming and its Impact on GPS Receivers

Dmitry Kuznetsov

Abstract: All smartphones today have a GNSS receiver on board and most smartphones also have an LTE modem. The LTE Standard [1] regulates bandwidths, power, bands and other parameters of the LTE signal. However, there are many different LTE bands, and some of the bands have the second harmonic of their frequency range very close to the GPS L1 band. For instance, the uplink channels of LTE Band 13 and 14 have the second harmonic of their central frequencies at 1564 MHz and 1586 MHz, respectively. Considering the maximum bandwidth of the channels, the transmitted signal may be located just a few megahertz away from the GPS L1 frequency band. This close proximity creates interference conditions ("LTE jamming" here and below) for a GNSS receiver every time an LTE modem transmits something. The maximum allowed transmission power is limited by 23 dBm. The LTE jamming power, which a GNSS receiver gets at its input, is much lower than that and determined by the antenna isolation and nonlinearity of the LTE transmitter power amplifier (PA), which creates the second harmonic of the signal. The absolute power of the LTE signal at the GNSS receiver input port significantly depends on these factors, which are specific for any modem and hardware design, but none of these parameters are ideal. In addition, the paper shows that, in some configurations, the LTE jammer may be located too close to the GPS L1 band to be rejected by a SAW filter. The resulting jamming can seriously degrade the performance of a GNSS receiver, creating position outliers and even loss of position fix. This paper shows the impact of the second harmonic of the LTE signal on the GPS receiver performance and gives recommendations to receiver designers to address that. The significance of this work lies in the determination of the GPS receiver SNR loss as a function of the LTE jamming parameters at the input. Importantly, this work also provides recommendations to GNSS receiver designers about selecting certain receiver design parameters. Note, however, that LTE jamming can adversely affect constellations other than the GPS system that is studied in this work.

Published in: Proceedings of the 35th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2022)
September 19 - 23, 2022
Hyatt Regency Denver
Denver, Colorado

Pages: 3915 - 3924

Cite this article: Kuznetsov, Dmitry, "Characterization of LTE Jamming and its Impact on GPS Receivers," *Proceedings of the 35th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2022)*, Denver, Colorado, September 2022, pp. 3915-3924.
https://doi.org/10.33012/2022.18574

LTE 妨害の特徴と GPS 受信機への影響

ドミトリー・クズネツォフ

現在のすべてのスマートフォンには GNSS 受信機が搭載されており、ほとんどのスマートフォンには LTE モデムも搭載されています。LTE 規格 [1] は、LTE 信号の帯域幅、電力、帯域、その他のパラメーターを規制します。ただし、LTE 帯域には多数の異なる帯域があり、一部の帯域では、その周波数範囲の第 2 高調波が GPS L1 帯域に非常に近いものがあります。たとえば、LTE バンド 13 と 14 のアップリンク チャネルには、それぞれ 1564 MHz と 1586 MHz に中心周波数の第 2 高調波があります。チャネルの最大帯域幅を考慮すると、送信信号は GPS L1 周波数帯域からわずか数メガヘルツ離れたところに位置する可能性があります。この近接により、LTE モデムが何かを送信するたびに、GNSS 受信機に干渉状態（以下の「LTE ジャミング」）が発生します。最大許容送信電力は 23 dBm に制限されます。GNSS 受信機が入力で取得する LTE 妨害電力はそれよりもはるかに低く、信号の 2 次高調波を生成する LTE 送信機のパワー アンプ（PA）のアンテナ分離と非線形性によって決まります。GNSS 受信機入力ポートにおける LTE 信号の絶対電力は、モデムやハードウェア設計に固有のこれらの要因に大きく依存しますが、これらのパラメータはどれも理想的ではありません。さらに、この論文は、一部の構成では、LTE ジャマーが GPS L1 帯域に近すぎて SAW フィルターで拒否できない可能性があることを示しています。結果として生じる妨害により、GNSS 受信機のパフォーマンスが大幅にパラメータの外れ値が発生して、位置の修正が失われることさえあります。このペーパーでは、LTE 信号の第 2 高調波が GPS 受信機のパフォーマンスに及ぼす影響を示し、それに対処するための推奨事項を受信機の設計者に提供します。この研究の重要性は、入力における LTE 妨害パラメータの関数として GPS 受信機の SNR 損失を決定することにあります。重要なのは、この研究では、特定の受信機設計パラメータの選択について GNSS 受信機設計者に推奨事項も提供していることです。ただし、LTE ジャミングは、この研究で研究している GPS システム以外のコンステレーションに悪影響を与える可能性があることに注意してください。

第 35 回航法研究所衛星部門国際技術会議（ION GNSS+ 2022）の議事録 2022 年
9 月 19 ～ 23 日
ハイアット リージェンシー デンバー
コロラド州デンバー

参考文献:

クズネツォフ、ドミトリー、「LTE 妨害の特性と GPS 受信機への影響」、航法研究所衛星部門の第 35 回国際技術会議（ION GNSS+ 2022）の議事録、コロラド州デンバー、2022 年 9 月、3915 ページ- 3924。
https://doi.org/10.33012/2022.18574

Time-Frequency Analysis of GNSS Jamming Events Detected on U.S. Highways

Sandeep Jada, John Bowman, Mark Psiaki, Chenming Fan, Mathieu Joerger

Abstract: In this paper, we implement jamming detectors designed for off-the-shelf GNSS receivers using publicly available data collected at more than 900 receiver locations during an eight-month-long period. We identify spatial and temporal patterns in the detected events to predict when and where jamming may occur. We find patterns that coincide with daily driver commutes and weekly delivery schedules along U.S. highways. We then validate this approach by developing a new Neyaman-Pearson locally-optimal signal power monitor using wideband radio-frequency (RF) data, and by deploying our own equipment at the locations and times of the predicted jamming. Two example wideband data sets are presented, which we collected in Colorado and Virginia. We analyze this data in the time-frequency domain and show interference in the GPS L1 band caused by recurring unidentified communication broadcasts and by personal privacy devices (PPDs).

Published in: Proceedings of the 35th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2022)
September 19 - 23, 2022
Hyatt Regency Denver
Denver, Colorado

Pages: 933 - 946

Cite this article: Jada, Sandeep, Bowman, John, Psiaki, Mark, Fan, Chenming, Joerger, Mathieu, "Time-Frequency Analysis of GNSS Jamming Events Detected on U.S. Highways," *Proceedings of the 35th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2022)*, Denver, Colorado, September 2022, pp. 933-946.
https://doi.org/10.33012/2022.18528

米国の高速道路で検出された GNSS 妨害イベントの時間周波数分析

サンディープ・ジェイダ、ジョン・ボウマン、マーク・サイアキ、チェンミン・ファン、マチュー・ジョルガー

このペーパーでは、8 か月間に 900 以上の受信機位置で収集された公開データを使用して、既製の GNSS 受信機用に設計された妨害検出器を実装します。検出されたイベントの空間的および時間的パターンを特定して、いつ、どこで妨害が発生するかを予測します。米国の高速道路では、毎日のドライバーの通勤と毎週の配達スケジュールと一致するパターンが見つかりました。次に、広帯域無線周波数（RF）データを使用して新しい**ネヤマン・ピアソン**の局所的に最適な信号パワー モニターを開発し、予測された妨害の場所と時間に独自の機器を展開することで、このアプローチを検証します。コロラド州とバージニア州で収集した 2つの広帯域データ セットの例を示します。このデータを時間周波数領域で分析し、繰り返し発生する身元不明の通信ブロードキャストと**パーソナル プライバシー デバイス（PPD）**によって引き起こされる GPS L1 帯域の干渉を示します。

ネヤマン-ピアソンに関する情報

”Neyman-Pearson”は統計学と検定理論において重要な概念であり、GPS の分野においても、信号処理や位置推定の文脈で関連している可能性があります。

Neyman-Pearson の基本的な概念は、2 つの異なる統計的モデルを比較し、それらの間でどれだけの証拠があるかを評価することです。特に、帰無仮説（通常は既知の状態やパラメータに関する仮説）と対立仮説（通常は何か新しい状態やパラメータに関する仮説）を比較します。

GPS の分野では、Neyman-Pearson の原理が信号の検出や位置推定などにどれだけの信頼性があるかを判断するために使用されることがあります。たとえば、GPS 信号の中に異常がある場合、それを検出し、正確な位置推定を行うために統計的手法が使用されることがあります。

第 35 回航法研究所衛星部門国際技術会議（ION GNSS+ 2022）の議事録 2022 年
9 月 19 ～ 23 日
ハイアット リージェンシー デンバー
コロラド州デンバー

An RF Front-End Optimal Selection Scheme for Reconfigurable Anti-Jamming Polarization-Sensitive Array with Application to GNSS

Yandong Sun, Jian Xie, Chuang Han, Ling Wang, Mingliang Tao

Peer Reviewed

Abstract: Polarization-sensitive array (PSA) can sense satellite signals from multiple dimensions and separate signals from interference according to various characteristics. Hence, the use of PSA improves the interference rejection capability of the global navigation satellite system (GNSS). Whereas it also brings a significant increase in computational complexity as there are more dimensions of array signal processing. Therefore, it is urgent to seek a method to employ fewer radiofrequency (RF) front-ends and antennas while still achieving superior anti-interference performance. In this paper, we investigate the influence of PSA configuration on interference suppression performance and propose an RF front-end optimal selection scheme for reconfigurable anti-jamming PSA with application to GNSS. Combining adaptive array processing algorithm and RF front-end selection strategy, we formulate the expression of the effective carrier to noise ratio (CNR) to analyze the performance enhancement generated by PSA reconfiguration. An approach is presented to solve the upper bound of the effective CNR to plot the trade-off curve between performance and cost, which can guide the selection of the optimal number of RF front-ends. Then another method is used to acquire the layout of the chosen optimal RF front-ends that can maximize the effective CNR. Numerical results illustrate the effectiveness and high efficiency of the proposed PSA reconfiguration scheme.

Published in: Proceedings of the 35th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2022)
September 19 - 23, 2022
Hyatt Regency Denver
Denver, Colorado

GNSS アプリケーションを備えた再構成可能な耐ジャミング偏波感応アレイのための RF フロントエンド最適選択スキーム

ヤンドン・スン、ジェン・シェ、チュアン・ハン、リン・ワン、ミンリャン・タオ

偏波感応アレイ（PSA：Polarization-sensitive array）は、衛星信号を多次元から感知し、さまざまな特性に従って信号を干渉から分離できます。したがって、PSA を使用すると、全地球航法衛星システム（GNSS）の干渉除去能力が向上します。一方、アレイ信号処理の次元が増えるため、計算の複雑さも大幅に増加します。したがって、優れた耐干渉性能を達成しながら、使用する無線周波数（RF）フロントエンドとアンテナの数を減らす方法を模索することが急務となっています。この論文では、PSA 構成が干渉抑制性能に及ぼす影響を調査し、GNSS に適用する再構成可能な耐ジャミング PSA のための RF フロントエンドの最適な選択方式を提案します。アダプティブ アレイ処理アルゴリズムと RF フロントエンド選択戦略を組み合わせて、有効搬送波対雑音比（CNR）の式を定式化し、PSA 再構成によって生成されるパフォーマンス向上を分析します。実効 CNR の上限を解決して、パフォーマンスとコストの間のトレードオフ曲線をプロットするアプローチを示します。これにより、最適な RF フロントエンド数の選択をガイドできます。次に、別の方法を使用して、実効 CNR を最大化できる、選択された最適な RF フロントエンドのレイアウトを取得します。数値結果は、提案された PSA 再構成スキームの有効性と高効率を示しています。

第 35 回航法研究所衛星部門国際技術会議（ION GNSS+ 2022）の議事録 2022 年
9 月 19 ～ 23 日
ハイアット リージェンシー デンバー
コロラド州デンバー

On the Impact of Jamming on Horizontal Protection Level and Integrity Assessment for Terrestrial Localization

Syed Ali Kazim, Nourdine Aït Tmazirte, Juliette Marais, Avag Tsaturyan

Peer Reviewed

Abstract: Localization function for an advanced intelligent transport system, such as an autonomous vehicle, must ensure various operational requirements such as safety, accuracy, availability and continuity of service, anytime, anywhere, at a reasonable cost. Global Navigation Satellite System (GNSS) have many advantages insofar as they present the most accessible technology to the user to determine its position with a certain accuracy without prior knowledge. However, in an environment where signal reception may not be optimal especially due to phenomena such as satellite blockage, multipath, intentional or unintentional interferences and spoofing, it becomes very challenging to meet all these requirements, especially those related to operational safety. The latter is measured by evaluating the integrity of the localization function. It can be evaluated through a Protection Level, which is calculated by the receiver to self-monitor its integrity, also called RAIM (Receiver Autonomous Integrity Monitoring). In the literature, integrity in presence of multipath and NLOS has been extensively investigated [1] as well interference detection and mitigation solutions [2]. However, the impact of interference presence and mitigation on integrity monitoring is not deeply addressed yet. In this study, we evaluate some key performance indicators (KPI's) for GNSS users. These indicators will be evaluated for three different cases; 1) when no interference is applied and clean GNSS signals are processed. 2) In the presence of interference but without any mitigation technique. 3) After applying a mitigation technique at the pre-correlation level to filter the interference signal. The mitigation technique relies on state-of-the-art Notch filters provided by a Septentrio receiver. The interference signals are generated in the laboratory to produce disturbances in the GNSS band. Thus, and thanks to the a priori knowledge of the true position, it is possible to establish the Stanford diagrams for these cases. A deep analysis of performance in the presence and absence of interferences and in the presence and absence of a mitigation technique allows the first conclusions to be drawn on the evolution of accuracy, availability and operational safety indicators. The preliminary results reveal the importance of considering, from the design phase of the localization function, the possibility of dealing with this phenomenon, in particular in the measurement weighting model to use for enhanced performance.

Published in: Proceedings of the 2022 International Technical Meeting of The Institute of Navigation
January 25 - 27, 2022
Hyatt Regency Long Beach
Long Beach, California

水平方向の保護レベルと地上位置特定のための完全性評価に対する妨害電波の影響について

サイード・アリ・カジム、ヌールディン・アイット・マジルテ、ジュリエット・マレ、アヴァグ・ツァトゥリアン

自動運転車などの高度インテリジェント交通システムの位置特定機能では、安全性、正確性、可用性、サービスの継続性などのさまざまな運用要件を、いつでも、どこでも、妥当なコストで確保する必要があります。全地球測位衛星システム（GNSS）は、事前知識がなくても一定の精度で位置を決定できる最もアクセスしやすいテクノロジーをユーザーに提供するという点で、多くの利点があります。しかし、特に衛星の妨害、マルチパス、意図的または非意図的な干渉、スプーフィングなどの現象により信号受信が最適化されない環境では、これらすべての要件、特に運用の安全性に関連する要件を満たすことが非常に困難になります。後者は、位置特定機能の完全性を評価することによって測定されます。これは、受信機がその整合性を自己監視するために計算する保護レベル（RAIM（Receiver Autonomous Integrity Monitoring）とも呼ばれます）を通じて評価できます。文献では、マルチパスおよび NLOS が存在する場合の整合性が広範囲に調査されており［1］、干渉検出および軽減ソリューション［2］も同様です。ただし、干渉の存在とその軽減が完全性モニタリングに及ぼす影響については、まだ深く検討されていません。この研究では、GNSS ユーザーのいくつかの主要業績評価指標（KPI）を評価します。これらの指標は 3 つの異なるケースに対して評価されます。（1）干渉が適用されず、クリーンな GNSS 信号が処理される場合。（2）干渉が存在するが、緩和技術がない場合。（3）干渉信号をフィルタリングするために相関前レベルで軽減技術を適用した後。この軽減技術は、Septentrio 受信機によって提供される最先端の Notch フィルターに依存しています。干渉信号は実験室で生成され、GNSS 帯域に妨害を引き起こします。したがって、真の位置に関するアプリオリな知識のおかげで、これらの場合のスタンフォード図を確立することが可能です。干渉の有無、および緩和技術の有無におけるパフォーマンスの詳細な分析により、精度、可用性、および運用上の安全性指標の進化に関する最初の結論を導き出すことができます。予備的な結果は、位置特定機能の設計段階から、特にパフォーマンスを向上させるために使用する測定重み付けモデルにおいて、この現象に対処する可能性を検討することの重要性を明らかにしています。

航海学会 2022 年国際技術会議議事録 2022 年 1 月 25 ～ 27 日
ハイアット リージェンシー ロングビーチ
カリフォルニア州ロングビーチ

Combining High Precision and Interference Resilient Positioning Using Spatial Filtering for Real-World Jamming Scenarios

Tobias Bamberg, Michael Meurer, Andriy Konovaltsev

Abstract: The high relevance of GNSS for positioning and timing in different applications increase the risk of (intended or unintended) radio interference (e.g., jamming or spoofing). One of the most sophisticated and efficient countermeasure against this threat is an antenna array, which can utilize a spatial filter to mitigate malevolent signals (e.g. by placing a spatial null in the direction of these signals). Using an antenna array together with carrier phase positioning (used for highly accurate and precise positioning like RTK or PPP) requires extra care, because the spatial filtering manipulates the incoming phase of the different antenna elements in order to form the interference free signal. In this paper we will propose and compare two different approaches to mitigate interference and simultaneously maintain a consistent carrier phase measurement. The first approach does not need any preliminary information about the antenna array (blind approach), while the second approach explicitly requires such information (deterministic approach). These approaches will be tested in two different real-world scenarios including a low and a high dynamic jamming scenario. The results show that both approaches are valuable in different situations. However, the deterministic approach performs better in a matter of accuracy and precision even with unprecise knowledge about the antenna pattern.

Published in: Proceedings of the 35th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2022)
September 19 - 23, 2022
Hyatt Regency Denver
Denver, Colorado

Pages: 2074 - 2089

Cite this article: Bamberg, Tobias, Meurer, Michael, Konovaltsev, Andriy, "Combining High Precision and Interference Resilient Positioning Using Spatial Filtering for Real-World Jamming Scenarios," *Proceedings of the 35th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2022)*, Denver, Colorado, September 2022, pp. 2074-2089.
https://doi.org/10.33012/2022.18330

実世界の妨害電波シナリオのための空間フィルタリングを用いた高精度かつ干渉に強い測位の組み合わせ

トビアス・バンベルク、ミヒャエル・ミューラー、アンドリー・コノヴァルツェフ

概要：様々なアプリケーションにおける測位とタイミングのための GNSS の高い関連性は、（意図的または非意図的な）電波干渉（例えば、妨害やスプーフィング）のリスクを増加させる。この脅威に対する最も洗練された効率的な対策の 1 つはアンテナアレイであり、空間フィルタを利用して悪意のある信号を軽減することができます（例えば、これらの信号の方向に空間ヌルを配置することによって）。アンテナアレイを搬送波位相測位（RTK や PPP のような高精度で正確な測位に使用）と共に使用する場合、空間フィルタリングが干渉のない信号を形成するために異なるアンテナエレメントの受信位相を操作するため、特に注意が必要です。この論文では、干渉を緩和し、同時に一貫した搬送波位相測定を維持するための 2 つの異なるアプローチを提案し、比較します。1 つ目のアプローチはアンテナアレイに関する事前情報を必要とせず（ブラインドアプローチ）、2 つ目のアプローチはそのような情報を明示的に必要とします（決定論的アプローチ）。これらのアプローチは、低ダイナミックジャミングシナリオと高ダイナミックジャミングシナリオを含む 2 つの異なる実世界シナリオでテストされる。結果は、両アプローチが異なる状況において価値があることを示している。しかし、決定論的アプローチの方が、アンテナパターンに関する正確な知識がない場合でも、精度と正確さの点で優れている。

第 35 回航法研究所衛星部門国際技術会議（ION GNSS+ 2022）の議事録 2022 年
9 月 19 ～ 23 日
ハイアット リージェンシー デンバー
コロラド州デンバー

Stress Testing of a Low-Cost GNSS RFI Monitor

Nicolas Roberto San Miguel, Yu-Hsuan Chen, Sherman Lo, Todd Walter, Dennis Akos

Peer Reviewed

Abstract: The Global Navigation Satellite System (GNSS) is an important tool that is vulnerable to both intentional and unintentional radio frequency interference (RFI). This work seeks to develop a low-cost GNSS RFI monitor to detect and classify interference in an area. We present multiple signal combination-based jamming and spoofing experiments and provide an analysis of the results. Several simulated short duration jamming tests are applied to both L1 and L2 signals with four types of jamming interference, including continuous wave, narrowband jamming; broadband, additive white Gaussian noise jamming; chirp interference; and pulsed-chirp interference. A lift-off spoofing experiment combines real-time GNSS signals using two receive-only antennas and a programmable attenuator. The signals are processed using a low-cost u-blox F9P receiver and various power and signal quality metrics are analyzed. Specifically, the carrier-to-noise ratio (C/N0), the automatic gain control (AGC), and spectral analyses are useful for both identifying interference and classifying types of interference. Differences in power metric responses are observed depending on the characteristics and waveform of the jamming interference. Analyzing the position solution in addition to power metric and signal quality monitoring is found to be especially insightful in detecting the presented spoofing scenario. Our results characterize how the u-blox F9P receiver measures the several types of RFI and show the advantages of monitoring multiple metrics when monitoring for interference.

Published in: Proceedings of the 35th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2022)
September 19 - 23, 2022
Hyatt Regency Denver
Denver, Colorado

Pages: 3463 - 3478

Cite this article: Miguel, Nicolas Roberto San, Chen, Yu-Hsuan, Lo, Sherman, Walter, Todd, Akos, Dennis, "Stress Testing of a Low-Cost GNSS RFI Monitor," *Proceedings of the 35th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2022)*, Denver, Colorado, September 2022, pp. 3463-3478.
https://doi.org/10.33012/2022.18447

低コストの GNSS RFI モニターのストレス テスト

ニコラス・ロベルト・サン・ミゲル、ユー・シュアン・チェン、シャーマン・ロー、トッド・ウォルター、デニス・エイコス

全地球航法衛星システム（GNSS）は、意図的および非意図的な無線周波数干渉（RFI）に対して脆弱な重要なツールです。この研究では、エリア内の干渉を検出して分類するための低コストの GNSS RFI モニターを開発することを目指しています。複数の信号の組み合わせに基づく妨害とスプーフィングの実験を紹介し、結果の分析を提供します。いくつかの模擬短時間妨害テストが、連続波、狭帯域妨害を含む 4 種類の妨害を伴う L1 信号と L2 信号の両方に適用されます。広帯域、加法性ホワイト ガウス ノイズ ジャミング。チャープ干渉。パルスチャープ干渉。リフトオフ スプーフィング実験では、2 つの受信専用アンテナとプログラム可能な減衰器を使用してリアルタイム GNSS 信号を組み合わせます。信号は低コストの u-blox F9P レシーバーを使用して処理され、さまざまな電力と信号品質のメトリクスが分析されます。具体的には、搬送波対雑音比（C/N0）、自動利得制御（AGC）、およびスペクトル分析は、干渉の特定と干渉の種類の分類の両方に役立ちます。妨害電波の特性や波形に応じて、パワーメトリック応答の違いが観察されます。電力メトリックと信号品質の監視に加えて位置ソリューションを分析することは、提示されたなりすましシナリオを検出する上で特に有益であることがわかります。私たちの結果は、u-blox F9P 受信機が数種類の RFI をどのように測定するかを特徴づけ、干渉を監視する際に複数のメトリックを監視する利点を示しています。

第 35 回航法研究所衛星部門国際技術会議 (ION GNSS+ 2022) の議事録 2022 年
9 月 19 ～ 23 日
ハイアット リージェンシー デンバー
コロラド州デンバー

Real-time Detection and Localization of GNSS Interference Source

Zixi Liu, Sherman Lo, Todd Walter, Juan Blanch

Peer Reviewed

Abstract: The growing dependence of critical and safety-of-life systems on GNSS makes the ability to rapidly detect and localize the presence of GNSS interference events increasingly important. Ground-based GNSS jammer detection can be used to detect local interference sources. However, this approach is limited by line of sight (LOS) and hence applying it to large areas is costly in both time and money. A complementary technique is to use airborne GNSS receiver data as provided by Automatic Dependent Surveillance—Broadcast (ADS-B). As these receivers are at altitude, their LOSs can cover a wide ground area. The drawback to this method is that ADS-B was not designed for this purpose and the messages contain limited information for the assessment of radio frequency interference (RFI). This paper develops and demonstrates an algorithm for real-time detection and localization of GNSS interference sources using ADS-B. We implement and demonstrate this capability using recorded ADS-B transmissions from known interference events. This paper demonstrates detection of an interference source within few minutes of the onset of transmission and identification of the location within small degrees of error in latitude and longitude. The algorithm does not require prior knowledge about the interference source, it only assumes the source has omnidirectional radiation with continuous transmission. The algorithm generates a probability map for possible locations of the RFI source. This information can then yield the most likely information of the interference source including location and transmitted power. This paper tested the algorithm on a recent interference event that occurred around Denver International Airport (KDEN). This incident resulted in multiple aircraft reporting loss of transponder function and ADS-B issues within 30 NM of KDEN. The tested result showed fast detection and identification of the interference threat.

Published in: Proceedings of the 35th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2022)
September 19 - 23, 2022
Hyatt Regency Denver
Denver, Colorado

GNSS 干渉源のリアルタイム検出と位置特定

ジーシー・リウ、シャーマン・ロー、トッド・ウォルター、フアン・ブランチ

重要なシステムや生命安全システムの GNSS への依存度が高まっているため、GNSS 干渉イベントの存在を迅速に検出して位置特定する機能がますます重要になっています。地上ベースの GNSS 妨害波検出を使用して、ローカルの干渉源を検出できます。ただし、このアプローチは見通し線（LOS）によって制限されるため、広いエリアに適用するには時間と費用の両方がかかります。補完的な手法は、Automatic Dependent Surveillance-Broadcast（ADS-B）によって提供される航空機 GNSS 受信機データを使用することです。これらの受信機は高度にあるため、LOS は広い地上エリアをカバーできます。この方法の欠点は、ADS-B がこの目的のために設計されていないことと、メッセージに含まれる無線周波数干渉（RFI）の評価用の情報が限られていることです。この論文では、ADS-B を使用した GNSS 干渉源のリアルタイム検出と位置特定のためのアルゴリズムを開発し、実証します。私たちは、既知の干渉イベントから記録された ADS-B 送信を使用してこの機能を実装し、実証します。この論文では、送信開始から数分以内に干渉源を検出し、緯度と経度のわずかな誤差内で位置を特定することを実証します。このアルゴリズムでは、干渉源に関する事前の知識は必要ありません。干渉源が連続送信による全方向放射を持っていることのみを前提としています。このアルゴリズムは、RFI 発信元の可能性のある場所の確率マップを生成します。この情報から、位置や送信電力など、干渉源の最も可能性の高い情報が得られます。この論文では、デンバー国際空港（KDEN）周辺で最近発生した干渉イベントに関するアルゴリズムをテストしました。この事故により、KDEN から 30 NM 以内で複数の航空機がトランスポンダー機能の喪失と ADS-B の問題を報告しました。テストの結果、干渉の脅威を迅速に検出および特定できることがわかりました。

第 35 回航法研究所衛星部門国際技術会議（ION GNSS+ 2022）の議事録 2022 年
9 月 19 ～ 23 日
ハイアット リージェンシー デンバー
コロラド州デンバー

From ICAO GNSS Interference Mask to Jamming Protection Area For Safe Civil Aviation Operation

Guillaume Novella, Christophe Macabiau, Axel Garcia-Pena, Anaïs Martineau, Pierre Ladoux, Philippe Estival, Olivier Troubet-Lacoste, Christian Fleury, Catherine Ronfle-Nadaud

Abstract: Jamming situations taking place as part of anti-drone struggle or military exercises are a threat for civil aviation. During these jamming operations, in order to protect civil aviation operations, segregation zones (also called protection zone in this article) are elaborated in which GNSS ICAO minimum requirements are not guaranteed. Segregation zones refer to the area, determined by the regulator, in which pilots are warned of a potential GNSS service failure because of the jamming. Currently, these protection areas are deduced from the ITU standardized interference mask but it appears that these protection areas are much larger than the observed impacted zone, highlighting thus the inefficiency of the current method. In this article, first a clarification on the interpretation of the interference mask is proposed, in order to explain the difference between the size of the protection zone and the impacted area. Second, a new method is proposed to compute a new protection zone, and this method estimates the true impacted zone considering local RFI situation. The main innovation of this new method is to take into account the situation of the jammer in terms of aeronautical interference level in its local surroundings. The main advantage of this method is the protection area size reduction while still guaranteeing that minimum GNSS ICAO requirements are respected.

Published in: Proceedings of the 34th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2021)
September 20 - 24, 2021
Union Station Hotel
St. Louis, Missouri

民間航空の安全な運航のための ICAO GNSS 干渉マスクから妨害波保護エリアまで

ギヨーム・ノヴェッラ、クリストフ・マカビオ、アクセル・ガルシア＝ペーニャ、アナイス・マルティノー、ピエール・ラドゥー、フィリップ・エスティヴァル、オリヴィエ・トルベ＝ラコステ、クリスチャン・フルーリー、カトリーヌ・ロンフル＝ナドー

反ドローン闘争や軍事演習の一環として発生する妨害行為は、民間航空にとって脅威です。これらの妨害作戦中、民間航空の運航を保護するために、GNSS ICAO の最低要件が保証されない隔離ゾーン（この記事では保護ゾーンとも呼ばれます）が綿密に設定されます。分離ゾーンとは、規制当局によって決定され、妨害波による GNSS サービス障害の可能性についてパイロットに警告されるエリアを指します。現在、これらの保護エリアは ITU 標準化された干渉マスクから推定されていますが、これらの保護エリアは観測された影響ゾーンよりもはるかに大きいようで、現在の方法の非効率性が浮き彫りになっています。この記事では、保護ゾーンと影響を受けるエリアのサイズの違いを説明するために、まず干渉マスクの解釈を明確にすることを提案します。第二に、新しい保護ゾーンを計算するための新しい方法が提案され、この方法は、ローカルの RFI 状況を考慮して真の影響を受けるゾーンを推定します。この新しい方法の主な革新点は、周囲の航空干渉レベルという観点から妨害電波の状況を考慮に入れることです。この方法の主な利点は、GNSS ICAO の最小要件が遵守されることを保証しながら、保護エリアのサイズを縮小できることです。

追記情報：ICAO とは

ICAO（国際民間航空機関）は、国際的な民間航空の安全性や効率性を確保するための専門機関です。国際連合の専門機関の一つであり、民間航空機関の国際的な標準や手順の策定、監視、推進を担当しています。ICAO は 1944 年に設立され、本部はモントリオールにあります。

標準と規則の策定: ICAO は、民間航空における標準や規則を策定し、これを加盟国に推奨します。これには、飛行手順、航法、通信、安全基準、環境への影響の削減などが含まれます。

民間航空機の登録と認定: ICAO は各国が保有する民間航空機の登録および認定手続きをサポートし、安全性や標準に基づく手順が遵守されていることを確認します。

航空機の通信および航法設備の標準化: ICAO は航空機の通信および航法に関する国際標準を確立し、これに基づいた航空機の装備が促進されます。これは、GPS や ADS-B（自動従属監視 - ブロードキャスト）などの技術も含まれます。

航空事故の調査と報告: 航空事故が発生した場合、ICAO は調査を行い、事故の原因や改善策を提案します。

第 34 回航法研究所衛星部門国際技術会議（ION GNSS+ 2021）の議事録 2021 年
9 月 20 ～ 24 日ミズーリ州
セントルイス ユニオン ステーション ホテル

Evaluation of PNT Situational Awareness Algorithms and Methods

Sandeep Jada, Mark Psiaki, Sean Landerkin, Steven Langel, Arthur Scholz, Mathieu Joerger

Abstract: This paper describes the design and evaluation of new GNSS jamming detection methods for position, navigation and timing (PNT) situational awareness (SA). These methods are intended for implementation over large networks of GNSS receivers. We focus on jamming threats caused by personal privacy devices (PPDs). We first derive two new jamming detection tests to identify events of simultaneous drops in C/N0 impacting all satellites in view. To limit the risk of false alerts, we develop an automated process to model satellite-specific and receiver-station-specific C/N0 measurement variations under jamming-free conditions. These models are then incorporated in our new detectors and evaluated using months of GPS L1 C/N0 data from continuously operating reference stations (CORS). Tens to hundreds of events are detected monthly at CORS sites located next to highways. To confirm that the detected events are caused by jamming, we analyze CORS data over multiple days at multiple locations, and find patterns in jamming schedules. In addition, we process ADS-B-reported aircraft receiver data during two known radio-frequency interference (RFI) events that also impacted CORS data.

Published in: Proceedings of the 34th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2021)
September 20 - 24, 2021
Union Station Hotel
St. Louis, Missouri

PNT 状況認識アルゴリズムと方法の評価

サンディープ・ジェイダ、マーク・サイアキ、ショーン・ランダーキン、スティーヴン・ラングル、アーサー・ショルツ、マチュー・ジョルガー

この論文では、位置、ナビゲーション、タイミング（PNT）状況認識（SA）のための新しい GNSS 妨害検出方法の設計と評価について説明します。これらの方法は、GNSS 受信機の大規模ネットワーク上での実装を目的としています。
私たちは、**個人用プライバシー デバイス（PPD）**によって引き起こされる妨害の脅威に焦点を当てています。まず、視野内のすべての衛星に影響を与える C/N0 の同時低下イベントを特定するための 2 つの新しい妨害検出テストを導き出します。誤報のリスクを制限するために、妨害波のない条件下で衛星固有および受信局固有の C/N0 測定変動をモデル化する自動プロセスを開発します。これらのモデルは当社の新しい検出器に組み込まれ、継続的に運用されている基準局（CORS）からの数か月にわたる GPS L1 C/N0 データを使用して評価されます。
高速道路の隣にある CORS サイトでは、毎月数十から数百のイベントが検出されます。検出されたイベントが電波妨害によって引き起こされたものであることを確認するために、複数の場所で数日間にわたる CORS データを分析し、電波妨害スケジュールのパターンを見つけます。さらに、CORS データにも影響を与えた 2 つの既知の無線周波数干渉（RFI）イベント中に、ADS-B によって報告された航空機受信機データを処理します。

第 34 回航法研究所衛星部門国際技術会議（ION GNSS+ 2021）の議事録 2021 年
9 月 20 ～ 24 日ミズーリ州
セントルイス ユニオン ステーション ホテル

Mitigation of Frequency-Hopped Tick Jamming Signals

Daniele Borio and Ciro Gioia

Peer Reviewed

Abstract: Global Navigation Satellite System (GNSS) jamming is an evolving technology where new modulations are progressively introduced in order to reduce the impact of interference mitigation techniques such as Adaptive Notch Filters (ANFs). The Standardisation of GNSS Threat reporting and Receiver testing through International Knowledge Exchange, Experimentation and Exploitation (STRIKE3) project recently described a new class of jamming signals, called tick signals, where a basic frequency tick is hopped over a large frequency range. In this way, discontinuities are introduced in the instantaneous frequency of the jamming signals. These discontinuities reduce the effectiveness of ANFs, which unable to track the jamming signal. This paper analyses the effectiveness of interference mitigation techniques with respect to frequency-hopped tick jamming signals. ANFs and Robust Interference Mitigation (RIM) techniques are analysed. From the analysis, it emerges that, despite the presence of frequency discontinuities, ANFs provide some margin against tick signals. However, frequency discontinuities prevent ANFs to remove all the jamming components and receiver operations are denied for moderate Jamming to Noise power ratio (J/N)values. RIM techniques are not affected by the presence of frequency discontinuities and significantly higher jamming power are sustained by the receiver when this type of techniques is adopted.

Published in: 2020 IEEE/ION Position, Location and Navigation Symposium (PLANS)
April 20 - 23, 2020
Hilton Portland Downtown
Portland, Oregon

周波数ホッピングされたティック妨害信号の軽減

ダニエレ・ボリオとチロ・ジョイア

全地球航法衛星システム（GNSS）ジャミングは、アダプティブ ノッチ フィルター（ANF）などの干渉軽減技術の影響を軽減するために、新しい変調が徐々に導入される進化するテクノロジーです。International Knowledge Exchange, Experimentation and Exploitation（STRIKE3）プロジェクトによる GNSS 脅威レポートと受信機テストの標準化では、最近、基本周波数ティックが広い周波数範囲にわたってホッピングされる、ティック信号と呼ばれる新しいクラスの妨害信号について説明しました。このようにして、妨害信号の瞬間周波数に不連続性が生じます。これらの不連続により、ANF の有効性が低下し、妨害信号を追跡できなくなります。この論文では、周波数ホッピングされたティック妨害信号に関する干渉軽減技術の有効性を分析します。ANF とロバスト干渉軽減（RIM）技術が分析されます。分析から、周波数の不連続性の存在にもかかわらず、ANF はティック信号に対してある程度のマージンを提供することがわかります。ただし、周波数の不連続性により、ANF はすべての妨害成分を除去できず、中程度の妨害対雑音電力比（J/N）値では受信機の動作が拒否されます。RIM 技術は周波数不連続の存在による影響を受けず、このタイプの技術が採用されると、受信機によって大幅に高い妨害電力が維持されます。

2020 IEEE/ION Position, Location and Navigation Symposium (PLANS)
2020 年 4 月 20 ～ 23 日
ヒルトン ポートランド ダウンタウン
オレゴン州ポートランド

Spoofing Threats: Reality Check, Impact and Cure

Wim De Wilde, Jan Van Hees, Gert Cuypers, Jan Dumon, Jean-Marie Sleewaegen, Bruno Bougard

Abstract: The last decade GPS was introduced into numerous applications for tracking of persons, vehicles and goods. This came along with the commercial availability of jamming devices. The chirp signals generated by these basic devices could affect GPS reception in large areas. The last few years many publications described effective methods to mitigate chirp jammers and commercial receivers became available which are resilient against this type of interference. While jammers simply block positioning, GPS spoofers attempt to take control of the positioning output, deceiving the end user. This is accomplished by sending counterfeit GPS signals into the GPS antenna. Spoofers can alter the tracks recorded by vehicle monitors and break geofences, which are commonly applied to restrict the area in which devices or people can operate. One example of this is the electronic monitoring of criminals. Spoofers also pose a risk to critical infrastructure, including power centrals, telecommunication networks and transportation systems, as they rely on GPS for precise timing. Counterfeiting GPS signals is a rather complex task. It involves the generation of multiple CDMA-modulated radio signals, which are delayed and Doppler shifted to represent the signal at the desired (artificial) user position. Until just a few years ago, GPS signal simulators were expensive devices designed for rack mounting. Hence, the use of spoofers by individuals or criminal organisations was not a realistic threat. This changed with the advent of compact software defined radio's (SDR), which build on the latest advancements in RF semiconductor technology. These affordable credit-card sized radios generate fully configurable RF signals. They receive digital samples from a laptop over a high-speed USB connection. Many SDR developments are driven by the open source community and since 2015, open source software can be downloaded from the internet for generating digital GPS signals. The software repository includes instructions to use it with the most common SDR's and its compilation is a trivial task for anyone with some programming background. We were able to set up the system in short time, spoofing the location reported by cell phones. The paper will first analyse the GPS signal produced by a common SDR. This includes power measurements and range predictions as well as clock stability and consistency of the imitated code and phase ranges. Subsequently the paper describes the impact of these well-accessible spoofers on various receiver types. We tested the spoofer on cell phones, on automotive grade receiver modules and on several high-accuracy receivers. The PolaRx5 receiver participating in the test offers a wide variety of signal quality outputs and a graphical user interface to display them in real time or during post-processing. This provides full visibility on the spoofer's behaviour. The tests cover a number of spoofing scenarios. In many vehicle tracking and geofencing attacks, the user has access to the GPS antenna. Authentic GNSS signals can be blocked and replaced with imitated signals. This is a first scenario in which receiver behaviour will be analysed, along with the impact of power levels and time offsets. If the antenna cannot be accessed, the spoofing signal needs to be superimposed on the genuine GNSS signal. As a first, crude approach, this can be achieved by simply connecting a transmit antenna to an SDR and overpowering the signal from space, with only coarse time synchronization. Note that, in principle, this attack could be detected by observing an unusual antenna referenced power spectral density. After analysing the receiver behaviour when affected by this basic spoofing approach, we will study a more sophisticated spoofing attack, in which the spoofer synchronises to GPS and gradually pulls the tracking channels away from the authentic signal. Once a receiver is tracking the spoofer signal, the transmit power could be lowered making the spoofer almost undetectable. This attack will be simulated using a commercial RF constellation simulator, which is capable to simulate this form of spoofing. Spoofing robustness of receivers depend on their ability to discriminate between an authentic signal and a counterfeit signal. This in turn depends on the quality of the counterfeiting. It will be pointed out that the cost and complexity of a spoofer rapidly increases with the number of signal features it is able to simulate. Septentrio receiver modules monitor many parameters, which could be used for authenticity assessment of the signal. They have grip on multiple components of the signal broadcasted by the satellite, clock behaviour and on signal propagation effects like multipath and ionospheric delay. Besides, they can also detect and mitigate complementary jammers. This enables the construction of a spoofing indication flag, which correctly reacts on any spoofing scenario of the earlier tests, including the sophisticated scenario.

Published in: Proceedings of the 30th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2017)
September 25 - 29, 2017
Oregon Convention Center
Portland, Oregon

過去 10 年間、GPS は人、車両、物品を追跡するための多くのアプリケーションに導入されました。これに伴い、妨害装置が市販されるようになりました。これらの基本的なデバイスによって生成されるチャープ信号は、広範囲の GPS 受信に影響を与える可能性があります。ここ数年、多くの出版物でチャープ妨害波を軽減する効果的な方法が記載されており、この種の干渉に強い商用受信機が入手できるようになりました。ジャマーは測位を単にブロックするだけですが、GPS スプーファーは測位出力を制御してエンド ユーザーを騙そうとします。これは、偽の GPS 信号を GPS アンテナに送信することで実現されます。スプーファーは、車両モニターによって記録された軌跡を改ざんし、デバイスや人が動作できるエリアを制限するために一般的に適用されるジオフェンスを破壊する可能性があります。その一例として、犯罪者の電子監視が挙げられます。スプーファーは正確なタイミングを GPS に依存しているため、電力中央局、通信ネットワーク、交通システムなどの重要なインフラにもリスクをもたらします。GPS 信号を偽造するのはかなり複雑な作業です。これには、複数の CDMA 変調無線信号の生成が含まれます。これらの信号は遅延され、ドップラー シフトされて、目的の（人工的な）ユーザー位置の信号を表します。ほんの数年前まで、GPS 信号シミュレーターはラックマウント用に設計された高価なデバイスでした。したがって、個人や犯罪組織によるスプーファーの使用は現実的な脅威ではありませんでした。この状況は、RF 半導体技術の最新の進歩に基づいて構築された小型ソフトウェア無線機（SDR）の出現によって変わりました。これらの手頃な価格のクレジット カード サイズの無線機は、完全に構成可能な RF 信号を生成します。高速 USB 接続を介してラップトップからデジタル サンプルを受信します。SDR 開発の多くはオープンソース コミュニティによって推進されており、2015 年以降、デジタル GPS 信号を生成するオープンソース ソフトウェアをインターネットからダウンロードできるようになりました。ソフトウェア リポジトリには、最も一般的な SDR でそれを使用するための手順が含まれており、そのコンパイルはプログラミングの経験がある人にとっては簡単な作業です。携帯電話からの位置情報を偽装し、短時間でシステムを構築することができた。この論文ではまず、一般的な SDR によって生成される GPS 信号を分析します。これには、クロックの安定性と、模倣されたコードと位相範囲の一貫性だけでなく、電力測定と範囲予測も含まれます。続いて、この論文では、これらのアクセスしやすいスプーファーがさまざまな種類の受信機に及ぼす影響について説明します。私たちは、携帯電話、自動車グレードの受信機モジュール、およびいくつかの高精度受信機でスプーファーをテストしました。テストに参加した PolaRx5 受信機は、さまざまな信号品質出力と、それらをリアルタイムまたは後処理中に表示するためのグラフィカル ユーザー インターフェイスを提供します。これにより、スプーファーの動作を完全に可視化できます。テストでは、多数のスプーフィング シナリオがカバーされています。多くの車両追跡攻撃やジオフェンシング攻撃では、ユーザーは GPS アンテナにアクセスできます。本物の GNSS 信号がブロックされ、模倣された信号に置き換えられる可能性があります。これは、受信機の動作が電力レベルと時間オフセットの影響とともに分析される最初のシナリオです。アンテナにアクセスできない場合は、本物の GNSS 信号にスプーフィング信号を重畳する必要があります。最初の粗雑なアプローチとして、これは単に送信アンテナを SDR に接続し、大まかな時間同期のみを使用して宇宙からの信号に電力を供給することで達成できます。原則として、この攻撃は、異常なアンテナ参照電力スペクトル密度を観察することによって検出できることに注意してください。この基本的なスプーフィング手法の影響を受けたときの受信機の動作を分析した後、スプーファーが GPS に同期し、追跡チャネルを本物の信

号から徐々に引き離す、より高度なスプーフィング攻撃を研究します。受信機がスプーファー信号を追跡すると、送信電力が低下し、スプーファーがほとんど検出されなくなる可能性があります。この攻撃は、この形式のスプーフィングをシミュレートできる市販の RF コンスタレーション シミュレータを使用してシミュレートされます。受信機のスプーフィング耐性は、本物の信号と偽造信号を区別する能力に依存します。これは偽造品の品質によって決まります。スプーファのコストと複雑さは、シミュレートできる信号特徴の数に応じて急速に増加することが指摘されます。Septentrio 受信機モジュールは多くのパラメータを監視し、信号の信頼性評価に使用できます。これらは、衛星によってブロードキャストされる信号の複数のコンポーネント、クロックの動作、およびマルチパスや電離層遅延などの信号伝播の影響を把握します。さらに、相補的な妨害電波を検出して軽減することもできます。これにより、高度なシナリオを含む、以前のテストのあらゆるスプーフィング シナリオに正しく反応するスプーフィング指示フラグの構築が可能になります。スプーファーは GPS と同期し、追跡チャネルを本物の信号から徐々に引き離します。受信機がスプーファー信号を追跡すると、送信電力が低下し、スプーファーがほとんど検出されなくなる可能性があります。この攻撃は、この形式のスプーフィングをシミュレートできる市販の RF コンスタレーション シミュレータを使用してシミュレートされます。受信機のスプーフィング耐性は、本物の信号と偽造信号を区別する能力に依存します。これは偽造品の品質によって決まります。スプーファのコストと複雑さは、シミュレートできる信号特徴の数に応じて急速に増加することが指摘されます。Septentrio 受信機モジュールは多くのパラメータを監視し、信号の信頼性評価に使用できます。これらは、衛星によってブロードキャストされる信号の複数のコンポーネント、クロックの動作、およびマルチパスや電離層遅延などの信号伝播の影響を把握します。さらに、相補的な妨害電波を検出して軽減することもできます。これにより、高度なシナリオを含む、以前のテストのあらゆるスプーフィング シナリオに正しく反応するスプーフィング指示フラグの構築が可能になります。スプーファーは GPS と同期し、追跡チャネルを本物の信号から徐々に引き離します。受信機がスプーファー信号を追跡すると、送信電力が低下し、スプーファーがほとんど検出されなくなる可能性があります。この攻撃は、この形式のスプーフィングをシミュレートできる市販の RF コンスタレーション シミュレータを使用してシミュレートされます。受信機のスプーフィング耐性は、本物の信号と偽造信号を区別する能力に依存します。これは偽造品の品質によって決まります。スプーファのコストと複雑さは、シミュレートできる信号特徴の数に応じて急速に増加することが指摘されます。Septentrio 受信機モジュールは多くのパラメータを監視し、信号の信頼性評価に使用できます。これらは、衛星によってブロードキャストされる信号の複数のコンポーネント、クロックの動作、およびマルチパスや電離層遅延などの信号伝播の影響を把握します。さらに、相補的な妨害電波を検出して軽減することもできます。これにより、高度なシナリオを含む、以前のテストのあらゆるスプーフィング シナリオに正しく反応するスプーフィング指示フラグの構築が可能になります。

第 30 回航法研究所衛星部門国際技術会議（ION GNSS+ 2017）の議事録 2017 年
9 月 25 ～ 29 日
オレゴン コンベンション センター
オレゴン州ポートランド

Blank page

Novel Replay Attacks Against Galileo Open Service Navigation Message Authentication

Haiyang Wang, Yuanyu Zhang, Yulong Shen, Jinxiao Zhu, Yin Chen, Xiaohong Jiang

Abstract: Open Service Navigation Message Authentication (OSNMA) serves as a critical security mechanism for the Galileo global navigation satellite system. At the core of OSNMA is a Timed Efficient Stream Loss-tolerant Authentication (TESLA) scheme, which generates a tag for each navigation message using a secret key and later discloses the key to receivers for authenticating the message-tag pair. Despite its great effectiveness against spoofing attacks, OSNMA's ability to resist replay attacks is questionable since the replayed signals containing authentic messages and tags may bypass the authentication under certain circumstances. This paper, for the first time, reveals two serious vulnerabilities of OSNMA: time synchronization (TS) and non-continuous message authentication (NCMA). TS is a mandatory requirement that specifies that the difference between a receiver's local reference time and the Galileo System Time (GST) extracted from Galileo signals does not exceed a given threshold. Exploiting this vulnerability, we propose a pre-startup replay (PreRep) attack, where Galileo signals are continuously recorded and replayed to a victim receiver before it starts up such that the TS requirement is satisfied and the receiver is locked to the replayed signals. NCMA means that OSNMA temporarily suspends the authentication process probably due to the reception of a broken message, tag or key, and restores the authentication after receiving a later-disclosed valid message-tag-key pair. Based on this vulnerability, we propose a post-startup replay (PosRep) attack, which conducts the replay attack after the victim receiver starts up such that the replayed signals break the currently receiving message-tag-key pair, deliberately suspending the authentication process, while subsequently-replayed signals can pass the authentication successfully as the message-tag-key pairs inside are valid. Finally, we conducted extensive experiments based on real-world OSNMA-integrated receivers and two software-defined radio (SDR) devices to demonstrate the feasibility of the proposed attacks.

Published in: Proceedings of the 36th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2023)
September 11 - 15, 2023
Hyatt Regency Denver
Denver, Colorado

Galileo オープン サービス ナビゲーション メッセージ認証に対する新たなリプレイ攻撃

王海陽、張元宇、沈裕龍、朱金暁、チェン・イン、ジャン・シャオホン

Open Service Navigation Message Authentication（OSNMA）は、Galileo 全地球航法衛星システムの重要なセキュリティ メカニズムとして機能します。OSNMA の中核となるのは、Timed Efficient Stream Loss-tolerant Authentication（TESLA）スキームです。このスキームは、秘密キーを使用して各ナビゲーション メッセージのタグを生成し、後でメッセージとタグのペアを認証するために受信者にキーを開示します。OSNMA はスプーフィング攻撃に対して優れた効果を発揮しますが、本物のメッセージとタグを含むリプレイ信号は特定の状況下で認証をバイパスする可能性があるため、リプレイ攻撃に抵抗する OSNMA の能力には疑問があります。この文書では、OSNMA の 2 つの重大な脆弱性、時刻同期（TS）と非連続メッセージ認証（NCMA）が初めて明らかにされました。TS は、受信機のローカル基準時間と Galileo 信号から抽出された Galileo システム時間（GST）との差が所定のしきい値を超えないことを指定する必須要件です。この脆弱性を悪用して、起動前リプレイ（PreRep）攻撃を提案します。この攻撃では、Galileo 信号が継続的に記録され、対象の受信機が起動する前に再生され、TS 要件が満たされ、受信機が再生された信号にロックされます。NCMA は、おそらく壊れたメッセージ、タグ、またはキーの受信が原因で OSNMA が認証プロセスを一時的に停止し、後で公開される有効なメッセージとタグとキーのペアを受信した後に認証を復元することを意味します。この脆弱性に基づいて、私たちは起動後リプレイ（PosRep）攻撃を提案します。これは、被害者の受信機が起動した後にリプレイ攻撃を実行し、リプレイされた信号によって現在受信しているメッセージ タグとキーのペアを破り、認証プロセスを意図的に中断します。一方、その後に再生される信号は、内部のメッセージ タグとキーのペアが有効であるため、認証を正常に通過できます。最後に、提案されたしました。

第 36 回航法研究所衛星部門国際技術会議（ION GNSS+ 2023）の議事録 2023 年
9 月 11 ～ 15 日
ハイアット リージェンシー デンバー
コロラド州デンバー

Development and Testing of a Low-Cost GPS RFI Emulation System

Kenneth Johnston

Abstract: This paper proposes a low-cost (less than $250 USD) emulation capability of low-power Global Positioning System (GPS) Radio Frequency Interference (RFI) that is representative of modernized GPS jammer waveforms and modulations. The proposed system is consistent with the US FCC and Industry Canada Spectrum Management policy and regulations while meeting the requirements of lab testing GPS RFI and assessing the impact on GPS receivers. During the past several years there has been a proliferation of Personal Privacy Devices (PPDs) that have been well documented in Institute of Navigation (ION) papers and through the STRIKE3 project in Europe. Many of these PPDs are of low quality and have minor impact on actual GPS positioning or timing reliant systems. In Canada, it is illegal to import, purchase, possess or operate a GPS jammer. High performance RF Signal Generators and Waveform Generators that are capable of emulating GPS RFI signals up to at least 10 dBm are typically used in the lab by governments and larger companies. For smaller businesses, academia and some research organizations, often the cost of such equipment exceeds available budgets. These policy and financial constraints present challenges for a segment of the GPS industry to develop and test GPS RFI detection and monitoring capabilities and to assess the impact of new RFI mitigation algorithms and techniques specifically designed to counter GPS RFI. During this research, GPS RFI signals were generated using a combination of low-cost wideband RF synthesizers, specifically RF evaluation boards and modules based on Analog Devices (AD) ADF4351 chip and a low-cost Direct Digital Synthesis FeelTech FY6300 Function/Arbitrary Waveform Generator. The equipment was configured to generate examples of GPS RFI including Continuous Wave (CW), multi-tone, stepped tone, chirp waveforms, pulsed, narrowband and wideband noise waveforms, and Pseudo Random Noise (PRN) waveforms that were tailored to closely match the relevant GPS RF spectrum but could be easily modified for other GNSS systems based on the needs of a user. The generated RFI waveforms were recorded for comparison using a Signal Hound USB SA44B spectrum analyzer and a low-cost Airspy R2 Software Defined Radio. The combination of the ADF4351 and the FY6300 effectively jammed a Ublox NEO-7N GNSS receiver using selected RFI waveforms.

Published in: Proceedings of the 2022 International Technical Meeting of The Institute of Navigation
January 25 - 27, 2022
Hyatt Regency Long Beach
Long Beach, California

低コストの GPS RFI エミュレーション システムの開発とテスト
ケネス・ジョンストン

この論文では、最新の GPS 妨害波形と変調を代表する、低電力全地球測位システム（GPS）無線周波数干渉（RFI）の低コスト（250 米ドル未満）エミュレーション機能を提案します。提案されたシステムは、米国 FCC およびカナダ産業省のスペクトル管理ポリシーおよび規制と一致しており、ラボでの GPS RFI テストの要件を満たし、GPS 受信機への影響を評価しています。過去数年間、パーソナル プライバシー デバイス（PPD）が急増しており、これはナビゲーション研究所（ION）の論文やヨーロッパの STRIKE3 プロジェクトを通じて詳しく文書化されています。これらの PPD の多くは低品質であり、実際の GPS 測位やタイミング依存システムにはわずかな影響を与えます。カナダでは、GPS 妨害機の輸入、購入、所有、操作は違法です。少なくとも 10 dBm までの GPS RFI 信号をエミュレートできる高性能 RF 信号発生器および波形発生器は、通常、政府や大企業によって研究室で使用されています。中小企業、学術機関、および一部の研究機関の場合、そのような機器のコストが利用可能な予算を超えることがよくあります。これらの政策と財政上の制約は、GPS 業界の一部にとって、GPS RFI 検出および監視機能を開発およびテストし、GPS RFI に対抗するために特別に設計された新しい RFI 軽減アルゴリズムと技術の影響を評価するという課題を提示しています。この研究では、低コストの広帯域 RF シンセサイザー、具体的にはアナログ デバイセズ（AD）ADF4351 チップをベースにした RF 評価ボードおよびモジュールと、低コストのダイレクト デジタル シンセシス FeelTech FY6300 関数/任意波形発生器の組み合わせを使用して、GPS RFI 信号が生成されました。 この装置は、連続波（CW）、マルチトーン、ステップ トーン、チャープ波形、パルス状、狭帯域および広帯域のノイズ波形、および擬似ランダム ノイズ（PRN）波形を含む GPS RFI の例を生成するように構成されています。関連する GPS RF スペクトルですが、ユーザーのニーズに基づいて他の GNSS システム用に簡単に変更できます。生成された RFI 波形は、Signal Hound USB SA44B スペクトラム アナライザーと低コストの Airspy R2 Software Defined Radio を使用して比較のために記録されました。ADF4351 と FY6300 の組み合わせは、選択された RFI 波形を使用して Ublox NEO-7N GNSS 受信機を効果的に妨害することができました。

航海学会 2022 年国際技術会議議事録 2022 年
1 月 25 ～ 27 日
ハイアット リージェンシー ロングビーチ
カリフォルニア州ロングビーチ

Improving GNSS Positioning by De-noising Consecutive Correlator Outputs Using Graph Fourier Transform Filtering

Yiran Luo, Naser El-Sheimy

Peer Reviewed

Abstract: Navigation and positioning with GNSS are ubiquitous in our daily lives. However, GNSS receivers are vulnerable to irregular incoming signals, so their positioning, navigation, and timing (PNT) performance are usually degraded, especially in urban areas. It is, therefore, essential to enhance the baseband of GNSS receivers to sufficiently adapt to and be robust to volatile environments. Correlator outputs are the elementary products from GNSS baseband signal processing. The navigation and positioning accuracy is highly related to the quality of the correlator outputs, which contain less sophisticated noise sources than the code and carrier errors produced by the traditional tracking loops. In that case, the baseband processor can estimate the actual time of arrival (TOA) more easily. In this work, we directly de-noise the complex correlator outputs in the consecutive time domain to produce more accurate pseudorange measurements in harsh environments. Graph signal processing (GSP) is more extraordinary in alleviating irregular noise power than traditional digital signal processing (DSP). Thus, the GSP is applied to optimize the raw graph signals formed with the correlator outputs varying with the time and code offset. Then, the irregular graph domain is processed with graph Fourier transform (GFT) by exploring the geometry structure of the network of correlator outputs. The proposed GFT filtering method for the consecutive complex correlator outputs is realized in a GNSS software-defined radio (SDR) processing the GPS L1 C/A signals. Then, static GPS intermediate frequency (IF) data are collected in an urban area to test the proposed SDR. The real-world experiments demonstrate that the baseband processing results can be de-noised more efficiently, and the positioning accuracy is improved by 65.3% compared to the traditional algorithm.

Published in: Proceedings of the 35th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2022)
September 19 - 23, 2022
Hyatt Regency Denver
Denver, Colorado

グラフフーリエ変換フィルタリングを使用し連続相関器出力のノイズを除去することで GNSS 測位を改善する

イーラン・ルオ、ナセル・エル・シェイミー

GNSS によるナビゲーションと測位は、私たちの日常生活のいたるところで行われています。ただし、GNSS 受信機は不規則な受信信号に対して脆弱であるため、特に都市部では、測位、ナビゲーション、およびタイミング (PNT) のパフォーマンスが通常低下します。したがって、不安定な環境に十分に適応し、堅牢になるように GNSS 受信機のベースバンドを強化することが不可欠です。相関器出力は、GNSS ベースバンド信号処理からの基本的な積です。ナビゲーションと測位の精度は相関器出力の品質に大きく関係しており、相関器出力には従来の追跡ループによって生成されるコードやキャリアのエラーほど高度ではないノイズ源が含まれています。その場合、ベースバンド プロセッサは実際の到着時刻 (TOA) をより簡単に推定できます。この研究では、連続時間領域で複雑な相関器出力のノイズを直接除去し、過酷な環境でより正確な擬似距離測定を生成します。グラフ信号処理 (GSP) は、従来のデジタル信号処理 (DSP) よりも、不規則なノイズ電力を軽減する点で優れています。したがって、GSP は、時間とコードオフセットとともに変化する相関器出力で形成された生のグラフ信号を最適化するために適用されます。次に、相関器出力のネットワークの幾何構造を探索することにより、不規則なグラフ ドメインがグラフフーリエ変換 (GFT) で処理されます。連続する複素相関器出力に対して提案された GFT フィルタリング方法は、GPS L1 C/A 信号を処理する GNSS ソフトウェア無線 (SDR) で実現されます。次に、都市部で静的な GPS 中間周波数 (IF) データが収集され、提案された SDR がテストされます。実際の実験では、ベースバンド処理結果のノイズをより効率的に除去でき、測位精度が従来のアルゴリズムと比較して 65.3% 向上することが実証されました。

第 35 回航法研究所衛星部門国際技術会議（ION GNSS+ 2022）の議事録 2022 年
9 月 19 ～ 23 日
ハイアット リージェンシー デンバー
コロラド州デンバー

Developing a Low-Cost, High Performance, SDR-Based Local Positioning System

Fernando Palafox, Lyndsay Ruane, Scott Palo, Dennis Akos

Abstract: This paper explored the development of software-defined radio (SDR) based alternative positioning, navigation and timing (PNT), independent of any Global Navigation Satellite System (GNSS) for use in GNSS-denied areas. A navigation signal architecture based on GPS L1C signal was designed and broadcasted on a network of SDR-based transmitters. Signals were processed by a moving receiver which used a MATLAB-based software receiver to successfully estimate changes in range to each of the transmitters.

Published in: Proceedings of the 34th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2021)
September 20 - 24, 2021
Union Station Hotel
St. Louis, Missouri

Pages: 3189 - 3196

Cite this article: Palafox, Fernando, Ruane, Lyndsay, Palo, Scott, Akos, Dennis, "Developing a Low-Cost, High Performance, SDR-Based Local Positioning System," *Proceedings of the 34th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2021)*, St. Louis, Missouri, September 2021, pp. 3189-3196.
https://doi.org/10.33012/2021.18085

低コスト、高性能、SDR ベースのローカル測位システムの開発

フェルナンド・パラフォックス、リンジー・ルアン、スコット・パロ、デニス・エイコス

このペーパーでは、GNSS が拒否された地域で使用するための、全地球航法衛星システム（GNSS）から独立した、ソフトウェア無線（SDR）ベースの代替測位、ナビゲーション、およびタイミング（PNT）の開発について検討しました。GPS L1C 信号に基づくナビゲーション信号アーキテクチャが設計され、SDR ベースの送信機のネットワーク上でブロードキャストされました。信号は、MATLAB ベースのソフトウェア受信機を使用した移動受信機によって処理され、各送信機までの距離の変化を推定することに成功しました。

第 34 回航法研究所衛星部門国際技術会議（ION GNSS+ 2021）の議事録 2021 年
9 月 20 ～ 24 日ミズーリ州
セントルイス ユニオン ステーション ホテル

Palafox、Fernando、Ruane、Lynsay、Palo、Scott、Akos、Dennis、「低コスト、高性能、SDR ベースのローカル測位システムの開発」、航法研究所衛星部門の第 34 回国際技術会議議事録（ION GNSS+ 2021）、ミズーリ州セントルイス、2021 年 9 月、3189 ～ 3196 ページ。
https://doi.org/10.33012/2021.18085

Anti-Spoofing Technique Against GPS Time and Position Attacks Based on Sparse Signal Processing

Junhwan Lee, Erick Schmidt, Nikolaos Gatsis, David Akopian

Abstract: In this paper, we present a cost-effective software-developed Global Positioning System (GPS) anti-spoofing approach against Time Synchronization Attacks (TSAs) and spatial spoofing. We portray two signal-level spoofing characteristics that are predominantly discovered in aforementioned attacks, namely, spoofing profiles and consistency of modifying signals. While the spoofing profiles, which basically describe the inflicting signal shapes affecting the GPS observables, have already been analyzed in our previous research with respect to attacks against timing, this paper still utilizes the idea, yet implements and showcases the applicability of spoofing profiles in position domain. The extension, in fact, brings the idea of joint TSA and spatial spoofing. To jointly consider the time and spatial domains, the pseudorange and range rate equations are linearized with a non-conventional method. An antispoofing technique capable of withstanding TSAs, spatial attacks on single coordinate, and joint attacks is developed for stationary receiver. To validate the proposed approach, we utilize pre-recorded authentic GPS signals in the TEXBAT database for data transmission, which are captured by the Software Defined Radio receiver developed at UTSA. The algorithm is validated in simulations introducing synthetic spoofing and compared against Weighted Least Squares.

Published in: Proceedings of the 34th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2021)
September 20 - 24, 2021
Union Station Hotel
St. Louis, Missouri

スパース信号処理に基づく GPS 時間および位置攻撃に対するスプーフィング防止技術

ジュンファン・リー、エリック・シュミット、ニコラス・ガツィス、デヴィッド・アコピアン

本論文では、時間同期攻撃（TSA）および空間スプーフィングに対して、費用対効果の高いソフトウェア開発の全地球測位システム（GPS）スプーフィング対策アプローチを紹介する。我々は、前述の攻撃で主に発見される 2 つの信号レベルのスプーフィング特性、すなわちスプーフィング・プロファイルと変更信号の一貫性を描写する。スプーフィング・プロファイルは、基本的に GPS の観測値に影響を与える信号の形状を記述するもので、タイミングに対する攻撃に関しては、すでに以前の研究で分析されています。この拡張により、TSA と空間スプーフィングを併用するアイデアがもたらされました。時間領域と空間領域を共同で考慮するために、擬似距離とレンジレートの方程式を従来とは異なる方法で線形化する。TSA、単一座標に対する空間攻撃、および共同攻撃に耐えることができるアンチスプーフィング技術を定常受信機に対して開発する。提案手法を検証するために、TEXBAT データベースに予め記録された本物の GPS 信号をデータ送信に利用し、UTSA で開発された SDR（ソフトウェア定義無線機）Software Defined Radio 受信機で捕捉する。アルゴリズムは、合成スプーフィングを導入したシミュレーションで検証され、重み付き最小二乗法と比較される。

第 34 回航法研究所衛星部門国際技術会議（ION GNSS+ 2021）の議事録 2021 年
9 月 20 ～ 24 日ミズーリ州
セントルイス ユニオン ステーション ホテル

A Flexible Replay Delay Control Method for GNSS Direct Meaconing Signal

Shunshun Shang, Hong Li, Yimin Wei, Mingquan Lu

Peer Reviewed

Abstract: In this paper, we introduce a flexible delay control method for the GNSS direct meaconing signal. Since GNSS has been playing an important role in human life, we need to pay attention to its security issues, especially spoofing attacks. In order to explore the corresponding anti-spoofing techniques, we should know more about spoofing methods so that we can study the characteristics of spoofing signals. As far as an encrypted GNSS signal is concerned, only the direct meaconer can generate the corresponding spoofing signal. In detail, the meaconer receives authentic signals from different directions and delays them with different delays, respectively. However, the delay control method has not yet been public, which restricts researchers to explore more efficient anti-spoofing methods. To this end, we introduce a flexible delay control method for meaconer based on the integer and fractional delay filters. In detail, the integer filter can delay the signal with an integer delay that is an integer multiple of sampling period, and the fractional filter can delay the signal by a fraction delay. We implement the fractional filter using the Farrow structure so that we only need to adjust one parameter in the filter if the replay delay changes. As a consequence, the delay control method is flexible and easy to implement on a hardware platform. We verify the introduced method by carrying out meaconing attacks against both the GNSS-SDR receiver and the GPS hardware receiver of our lab.

Published in: Proceedings of the 2020 International Technical Meeting of The Institute of Navigation
January 21 - 24, 2020
Hyatt Regency Mission Bay
San Diego, California

GNSS 直接測定信号の柔軟な再生遅延制御方法

シャン・シュンシュン、ホン・リー、ウェイ・イーミン、ルー・ミンクアン

本稿では、GNSS 直接測定信号の柔軟な遅延制御方法を紹介します。GNSS は人間の生活において重要な役割を果たしているため、そのセキュリティ問題、特になりすまし攻撃に注意を払う必要があります。対応するスプーフィング対策技術を調査するには、スプーフィング信号の特性を研究できるように、スプーフィング手法についてさらに知る必要があります。暗号化された GNSS 信号に関する限り、対応するスプーフィング信号を生成できるのは直接測定者だけです。詳細には、ミーコナーはさまざまな方向から本物の信号を受信し、それぞれ異なる遅延でそれらを遅延させます。ただし、遅延制御方法はまだ公開されていないため、研究者はより効率的なスプーフィング対策方法を検討することが制限されています。この目的を達成するために、整数遅延フィルターと分数遅延フィルターに基づいた ミーコナーmeaconer の柔軟な遅延制御方法を導入します。詳細には、整数フィルターはサンプリング周期の整数倍である整数遅延で信号を遅延させることができ、分数フィルターは分数遅延で信号を遅延させることができます。Farrow 構造を使用してフラクショナル フィルターを実装するため、再生遅延が変化した場合にフィルター内の1つのパラメータを調整するだけで済みます。結果として、遅延制御方法は柔軟であり、ハードウェア プラットフォーム上での実装が容易です。私たちは、研究室の GNSS-SDR 受信機と GPS ハードウェア受信機の両方に対してミーコン攻撃を実行することで、導入された方法を検証します。

航海学会の 2020 年国際技術会議議事録 2020 年
1 月 21 ～ 24 日
ハイアット リージェンシー ミッション ベイ
サンディエゴ、カリフォルニア州

High-resolution Correlator Based Detection of GPS Spoofing Attacks Using the LASSO

Erick Schmidt, Nikolaos Gatsis, David Akopian

Peer Reviewed

Abstract: This work proposes a novel sparsity-based decomposition method for the correlator output signals in GPS receivers capable of detecting spoofing attacks. We model complex correlator outputs of the received signal to form a dictionary of triangle-shaped replicas and employ a sparsity technique that selects potential matching triangle replicas from said dictionary. We formulate an optimization problem at the receiver correlator domain by using the Least Absolute Shrinkage and Selection Operator (LASSO) to find sparse code-phase peaks where such triangle-shaped delays are located. The optimal solution of this optimization technique discriminates two different code-phase values as authentic and spoofed peaks in a sparse vector output. We use a threshold to mitigate false alarms. Additionally, we present an expansion of the model by enhancing the dictionary to a collection of shifted triangles with higher resolution. Our experiments are able to discriminate authentic and spoofer peaks from synthetic GPS-like simulations. We also test our method on a real dataset, namely the Texas Spoofing Test Battery (TEXBAT). Our method achieves less than 1% detection error rate (DER) in nominal signal-to-noise ratio (SNR) conditions.

Published in: 2020 IEEE/ION Position, Location and Navigation Symposium (PLANS)
April 20 - 23, 2020
Hilton Portland Downtown
Portland, Oregon

LASSO を使用した高解像度相関器ベースの GPS スプーフィング攻撃の検出

エリック・シュミット、ニコラオス・ガツィス、デヴィッド・アコピアン

この研究では、スプーフィング攻撃を検出できる GPS 受信機の相関器出力信号に対する新しいスパース性に基づく分解方法を提案します。受信信号の複雑な相関器出力をモデル化して三角形のレプリカの辞書を形成し、その辞書から一致する可能性のある三角形のレプリカを選択するスパース技術を採用します。最小絶対収縮選択演算子（LASSO）を使用して受信機相関器ドメインで最適化問題を定式化し、そのような三角形の遅延が位置するまばらなコード位相ピークを見つけます。この最適化手法の最適解は、スパース ベクトル出力内の 2 つの異なるコード位相値を本物のピークとスプーフィングされたピークとして識別します。しきい値を使用して誤報を軽減します。さらに、辞書をより高い解像度でシフトされた三角形のコレクションに拡張することによるモデルの拡張を示します。私たちの実験では、合成 GPS のようなシミュレーションから本物のピークとなりすましのピークを区別することができます。また、実際のデータセット、つまり Texas Spoofing Test Battery（TEXBAT）でメソッドをテストします。私たちの方法は、公称信号対雑音比（SNR）条件で 1% 未満の検出誤り率（DER）を達成します。

最小絶対収縮選択演算子（LASSO）は、統計学や機械学習の分野で用いられる変数選択および正則化手法の一つです。LASSOは、回帰分析において、予測に寄与する変数の数を減らし、かつモデルの複雑性を抑制するために使用されます。

LASSOの基本的なアイデアは、目的関数にペナルティ項を導入し、そのペナルティが非ゼロの係数を推定する際に影響を与えるようにすることです。通常、LASSOの目的関数は以下のように表されます：

$$\text{minimize}_{\beta_0,\beta} \left\{ \frac{1}{2n} \sum_{i=1}^{n} (y_i - \beta_0 - x_i^T \beta)^2 + \lambda \sum_{j=1}^{p} |\beta_j| \right\}$$

ここで：

y_i は観測された応答変数（目的変数），
x_i は対応する説明変数のベクトル，
β_0 は切片項，
β は説明変数の係数ベクトル，
n はサンプル数，
p は説明変数の数，
λ はL1ペナルティの強さを制御する調整パラメータです。

2020 IEEE/ION Position, Location and Navigation Symposium（PLANS）
2020 年 4 月 20 ～ 23 日 ヒルトン ポートランド ダウンタウン　オレゴン州ポートランド

Deeply Coupled Integration of a Software Defined GNSS Receiver and a Vibratory MEMS Rate Gyroscope Based Software Defined IMU

Baoyu Liu, Kaixiang Tong, Yang Gao

Abstract: In the ultra-tight integration, the signal processing of GNSS receiver baseband can be enhanced by the aiding of INS information. With the purpose of improving the performance of ultra-tight integration with low-cost MEMS (Micro-Electro-Mechanical System) IMU (Inertial Measurement Unit), the paper explores a deeply coupled integration scheme of GNSS and the software defined IMU (SDI) based on vibratory MEMS rate gyroscope. The error of vibratory MEMS rate gyroscope demodulated by peak detection technique is interpreted in the gyroscope signal domain and the gyroscope demodulation parameter deviations are estimated by the integration filter and adjusted accordingly. The presented integration scheme is tested by an integrated navigation system which consists of a software defined GNSS receiver, a single-axis vibratory MEMS gyroscope GI-CVG-N2100A based SDI and an Xsens MEMS IMU. The single-axis vibratory MEMS gyroscope GI-CVG-N2100A in the test, is employed to replace one of the gyroscope axes of the Xsens MEMS IMU.

Published in: Proceedings of the 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2020)
September 21 - 25, 2020

Pages: 3155 - 3162

Cite this article: Liu, Baoyu, Tong, Kaixiang, Gao, Yang, "Deeply Coupled Integration of a Software Defined GNSS Receiver and a Vibratory MEMS Rate Gyroscope Based Software Defined IMU," *Proceedings of the 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2020)*, September 2020, pp. 3155-3162.
https://doi.org/10.33012/2020.17710

ソフトウェア定義の GNSS 受信機と振動 MEMS レート ジャイロスコープ ベースのソフトウェア定義 IMU の密結合統合

バオユー・リウ、カイシャン・トン、ヤン・ガオ

ウルトラ・タイト・インテグレーションでは、GNSS 受信機のベースバンドの信号処理は、INS 情報の支援によって強化することができます。低コスト MEMS(Micro-Electro-Mechanical System)IMU(Inertial Measurement Unit)との超タイト統合のパフォーマンスを向上させる目的で、本論文では、振動 MEMS レートジャイロスコープに基づく GNSS とソフトウェア定義 IMU(SDI)の深い結合統合スキームを探求します。ピーク検出技術によって復調された振動 MEMS レートジャイロの誤差はジャイロ信号領域で解釈され、ジャイロ復調パラメータの偏差は統合フィルタによって推定され、それに応じて調整されます。ソフトウェア GNSS 受信機、1 軸振動 MEMS ジャイロスコープ GI-CVG-N2100A ベースの SDI、および X フィルタ MEMS IMU で構成される統合ナビゲーションシステムで、この統合スキームをテストしました。単軸振動 MEMS ジャイロスコープ GI-CVG-N2100A は、Xsens MEMS IMU のジャイロスコープ軸の 1 つを置き換えるために採用されています。

第 33 回航法研究所衛星部門国際技術会議（ION GNSS+ 2020）議事録
2020 年 9 月 21 ～ 25 日

GNSS Anti-jam RF-to-RF On Board Unit for ERTMS Train Control

Cosimo Stallo, Pietro Salvatori, Andrea Coluccia, Alessandro Neri, Francesco Rispoli, Massimiliano Ciaffi

Abstract: The GNSS technology has been selected as the key player for the modernization of the European Railways Train Management System (ERTMS). The main advantage of the satellite system is the possibility to realise cost-effective solutions able to increase the capacity and better allocate the railway resources. This cost reduction needs be performed without compromising the system safety that shall remain at the same level guarantee with the traditional systems. One of the problems that has to be accounted dealing with the GNSS is the Radio frequency interference like the intentional and not intentional. The presence of a jamming signal can degrade the performance of a GNSS location determination system and, if the ratio among the jammer is much higher the genuine signal, there could be a denial of service. One of the possible techniques able to mitigate such an issue is represented by the beamforming. In essence, having a CRPA (Controlled Reception Pattern Antenna) it is possible to identify the presence of the jamming signal and, eventually, combine the antennas' output to generate a signal that reduces the impact of such a treat. Particularly, in this work, we focused on a solution based on a four channel antenna processing chains constituted by a four element squared phased array and a 4 coherent channels front-end. The digital streams spilled after the ADCs (Analogue to Digital Converter) are the processed to identify the presence of a jamming signal. If the jamming signal is identified, then the processing unit will estimate the weights to implement a spatial filter able to minimize the impact of the jammer. The signal reconstructed after the beamformer is the put as input to a COTS/SDR receiver, making smoother the integration of this component in the navigation unit. The digital beamforming platform is designed to operate on scenarios typical of the railway environment. In this work we show the platform performance assessment of RF-2-RF GNSS anti-jam platform in terms of jamming detection and mitigation capabilities in presence of different attack scenarios potentially occurring in the ERTMS operative conditions. Particularly, we report the results of a test campaign by using Spirent tools, showing the capabilities of the anti-jam platform able to estimate the jammer direction of arrival, mitigate it cleaning the useful SIS (Signal in Space) from it and re-transmit it to a COTS/SDR receiver. The signal in output from these tools have been recorded by a four coherent channel frontend and then elaborated in postprocessing with the algorithms running on the platform. This approach has been selected to guarantee the possibility to inject the front-end with signals that have the same phase shifts and attenuations that would have been experimented on the field with the given array geometry and element beam patterns.

Published in: Proceedings of the 2020 International Technical Meeting of The Institute of Navigation
January 21 - 24, 2020
Hyatt Regency Mission Bay
San Diego, California

ERTMS 列車制御用の GNSS アンチジャム RF-to-RF 車載ユニット

コジモ・スタッロ、ピエトロ・サルバトーリ、アンドレア・コルッチャ、アレッサンドロ・ネーリ、フランチェスコ・リスポリ、マッシミリアーノ・チャッフィ

GNSS テクノロジーは、欧州鉄道列車管理システム（ERTMS）の近代化の主要な役割として選ばれました。衛星システムの主な利点は、容量を増やし、鉄道リソースをより適切に割り当てることができる、費用対効果の高いソリューションを実現できることです。このコスト削減は、従来のシステムと同レベルの保証を維持するシステムの安全性を損なうことなく実行する必要があります。GNSS を扱う際に考慮しなければならない問題の 1 つは、意図的なものとそうでないものにかかわらず、無線周波数の干渉です。妨害信号の存在により、GNSS 位置特定システムのパフォーマンスが低下する可能性があり、妨害信号間の比率が本物の信号よりもはるかに高い場合、サービス妨害が発生する可能性があります。このような問題を軽減できる技術の 1 つは、ビームフォーミングに代表されます。基本的に、CRPA（制御受信パターン アンテナ）を使用すると、妨害信号の存在を識別し、最終的にはアンテナの出力を組み合わせて、そのような扱いの影響を軽減する信号を生成することができます。特に、この研究では、4 つの要素の方形フェーズド アレイと 4 つのコヒーレント チャネル フロントエンドで構成される 4 チャネル アンテナ処理チェーンに基づくソリューションに焦点を当てました。ADC（アナログ - デジタル コンバーター）の後に流出したデジタル ストリームは、妨害信号の存在を識別するために処理されます。妨害信号が特定された場合、処理ユニットは重みを推定して、妨害信号の影響を最小限に抑えることができる空間フィルターを実装します。ビームフォーマーの後に再構築された信号は COTS/SDR レシーバーへの入力として入力され、ナビゲーション ユニットへのこのコンポーネントの統合がよりスムーズになります。デジタル ビームフォーミング プラットフォームは、鉄道環境に特有のシナリオで動作するように設計されています。この研究では、ERTMS の動作条件で潜在的に発生するさまざまな攻撃シナリオの存在下での妨害検出および軽減機能の観点から、RF-2-RF GNSS アンチ妨害プラットフォームのパフォーマンス評価を示します。特に、Spirent ツールを使用したテスト キャンペーンの結果を報告します。これは、妨害電波の到来方向を推定し、妨害電波を軽減し、有益な SIS（Signal in Space）を妨害電波から除去し、再送信できるアンチジャム プラットフォームの機能を示しています。 COTS/SDR 受信機に送信します。これらのツールからの出力信号は、4 つのコヒーレント チャネル フロントエンドによって記録され、プラットフォーム上で実行されるアルゴリズムによる後処理で精緻化されています。このアプローチは、特定のアレイ形状と要素ビーム パターンを使用して現場で実験されたものと同じ位相シフトと減衰を持つ信号をフロントエンドに注入する可能性を保証するために選択されました。

航海学会の 2020 年国際技術会議議事録 2020 年
1 月 21 ～ 24 日
ハイアット リージェンシー ミッション ベイ
サンディエゴ、カリフォルニア州

Performance Analysis of Low SWaP-C Jamming Mitigation Methods for Commercial Applications

Scott Burchfield, Scott Martin, David Bevly, Joshua Starling

Abstract: With the growing reliance upon GPS in the civilian sector, GPS need to be resilient to accidental and intentional interference threats. The Newark Airport incident, COTS PPDs, and other cases are prime examples of the need for resilient PNT in the civilian market. This paper implements four low SWaP-C (size, weight, power, and cost) mitigation methods and compares them in an attempt to determine the best algorithm for assured PNT. The algorithms analyzed are wavelet-implemented adaptive notch filter (WANF), SVD based FIR power minimization, space-time adaptive processing (STAP), and adaptive noise canceling. The first two algorithms use a signal antenna, and last two algorithms use two antennas. The algorithms are compared against an array of jamming scenarios, all of which originate from 3 main jamming types: continuous wave (CW) tone, narrowband noise, and chirp. The comparison between algorithms is quantified by analytical carrier to noise power density(CC/NN0) degradation at different jammer to signal (JJ/SS) power ratios and center frequency offsets, bandwidths, and sweep rates. The “mitigated” signal data is processed with a GPS L1 C/A receiver, and the receiver’s signal tracking CC/NN0 estimate is used to validate the analytical solutions. The analytical solution holds true for the wavelet implemented algorithm, the SVD based algorithm and the spacetime adaptive processing algorithm, but breaks down for the adaptive noise canceling algorithm. The results are analyzed and the conclusions are drawn based on the results.

Published in: Proceedings of the 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2020)
September 21 - 25, 2020

商用アプリケーション向けの低 SWaP-C 妨害波軽減法のパフォーマンス分析

スコット・バーチフィールド、スコット・マーティン、デヴィッド・ベブリー、ジョシュア・スターリング

民間部門における GPS への依存度が高まっているため、GPS は偶発的および意図的な干渉の脅威に対する耐性を備えている必要があります。ニューアーク空港事件、COTS PPD、およびその他の事件は、民間市場における回復力のある PNT の必要性を示す代表的な例です。このペーパーでは、保証された PNT に最適なアルゴリズムを決定するために、4 つの低 SWaP-C（サイズ、重量、電力、およびコスト）軽減方法を実装し、それらを比較します。分析されるアルゴリズムは、ウェーブレット実装の適応ノッチ フィルター（WANF）、SVD ベースの FIR 電力最小化、時空間適応処理（STAP）、および適応ノイズ キャンセリングです。最初の 2 つのアルゴリズムは信号アンテナを使用し、最後の 2 つのアルゴリズムは 2 つのアンテナを使用します。アルゴリズムは一連の妨害シナリオと比較されます。これらの妨害シナリオはすべて、連続波（CW）トーン、狭帯域ノイズ、チャープという 3 つの主要な妨害タイプに起因します。アルゴリズム間の比較は、さまざまな妨害波対信号（JJ/SS）電力比、中心周波数オフセット、帯域幅、掃引速度での搬送波対雑音電力密度（CC/NN0）の劣化を分析することによって定量化されます。「軽減された」信号データは GPS L1 C/A 受信機で処理され、受信機の信号追跡 CC/NN0 推定値が分析ソリューションの検証に使用されます。
この分析ソリューションは、ウェーブレット実装アルゴリズム、SVD ベースのアルゴリズム、時空適応処理アルゴリズムには当てはまりますが、**適応ノイズ キャンセリング アルゴリズム**では機能しません。結果が分析され、結果に基づいて結論が導き出されます。

第 33 回航法研究所衛星部門国際技術会議（ION GNSS+ 2020）議事録
2020 年 9 月 21 ～ 25 日

GNSS Software Defined Radio: History, Current Developments, and Standardization Efforts

Dennis Akos, Javier Arribas, M. Zahidul H. Bhuiyan, Pau Closas, Fabio Dovis, Ignacio Fernandez-Hernandez, Carles Fernández–Prades, Sanjeev Gunawardena, Todd Humphreys, Zaher M. Kassas, José A. López Salcedo, Mario Nicola, Thomas Pany, Mark L. Psiaki, Alexander Rügamer, Young-Jin Song, Jong-Hoon Won

Abstract: Taking the work conducted by the Global Navigation Satellite System (GNSS) Software Defined Radio (SDR) working group during the last decade as a seed, this contribution summarizes for the first time the history of GNSS SDR development. It highlights selected SDR implementations and achievements that are available to the public or influenced the general SDR development. The relation to the standardization process of Intermediate Frequency (IF) sample data and metadata is discussed, and a recent update of the Institute of Navigation (ION) SDR standard is recapitulated. The work focuses on GNSS SDR implementations on general purpose processors and leaves aside developments conducted on Field Programmable Gate Array (FPGA) and Application-Specific Integrated Circuits (ASICs) platforms. Data collection systems (i.e., front-ends) have always been of paramount importance for GNSS SDRs and are thus partly covered in this work. The work represents the knowledge of the authors but is not meant as a complete description of SDR history. Part of the authors plan to coordinate a more extensive work on this topic in the near future.

Published in: Proceedings of the 35th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2022)
September 19 - 23, 2022
Hyatt Regency Denver
Denver, Colorado

GNSS ソフトウェア無線: 歴史、現在の開発、および標準化の取り組み

デニス・アコス、ハビエル・アリバス、M・ザヒドゥル・H・ブイヤン他多数

過去 10 年間に全地球航法衛星システム（GNSS）ソフトウェア無線（SDR）ワーキング グループによって行われた作業をシードとして、この寄稿は GNSS SDR 開発の歴史を初めて要約します。一般に公開されている、または一般的な SDR 開発に影響を与えた、厳選された SDR の実装と成果に焦点を当てています。中間周波数（IF）サンプル データとメタデータの標準化プロセスとの関係について説明し、航法研究所（ION）SDR 標準の最近の更新について概説します。この作業は、汎用プロセッサでの GNSS SDR 実装に焦点を当てており、フィールド プログラマブル ゲート アレイ（FPGA）および特定用途向け集積回路（ASIC）プラットフォームで行われる開発は脇に置いています。データ収集システム（つまり、フロントエンド）は常に GNSS SDR にとって最も重要であるため、この作業で部分的に取り上げられます。この作品は著者の知識を表していますが、SDR の歴史を完全に説明するものではありません。著者の一部は、近い将来、このテーマに関するより広範な研究を調整する予定である。

第 35 回航法研究所衛星部門国際技術会議（ION GNSS+ 2022）の議事録 2022 年
9 月 19 ～ 23 日
ハイアット リージェンシー デンバー
コロラド州デンバー

Effect of Signal Quantization on Robust Anti-jamming in Snapshot Receivers

Helena Calatrava, Adrià Gusi-Amigó, Floor Melman, Pau Closas

Peer Reviewed

Abstract: GNSS jamming signals are L-band spectrum interferences that can jeopardize the operation of GNSS-based services. Consequently, jamming cancellation and mitigation techniques have received substantial interest in the field of GNSS positioning in the last few years. An advantageous approach to performing jamming mitigation relies on the use of robust statistics, with a framework known as Robust Interference Migration (RIM). In this paper, the RIM methodology is assessed in the context of a GNSS software snapshot receiver architecture under the presence of three jamming interferences simulated as representative cases of common mass-market jammers. A study on the effect of signal quantization in GNSS snapshot receivers is provided with a focus on interference mitigation. Results suggest that the clipping effect originated by the finite quantization dynamic range causes signal distortion, which leads to undesirable receiver performance for a low number of quantization bits. However, when applying RIM, a gain proportional to the number of quantization bits is observed in terms of the number of visible satellite vehicles, availability of the position, velocity and time (PVT) solution, and observed carrier-to-noise density ratio.

Published in: Proceedings of the 36th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2023)
September 11 - 15, 2023
Hyatt Regency Denver
Denver, Colorado

スナップショット受信機における堅牢なアンチジャミングに対する信号量子化の影響

ヘレナ カラトラバ、アドリア グシ アミーゴ、フロア メルマン、パウ クロサス

GNSS 妨害信号は、GNSS ベースのサービスの運用を危険にさらす可能性のある L バンドスペクトル干渉です。そのため、ここ数年、GNSS 測位の分野では、妨害信号のキャンセルと緩和技術が大きな関心を集めています。妨害波の緩和を実行する有利なアプローチは、ロバスト干渉マイグレーション（RIM）として知られるフレームワークによるロバスト統計の使用に依存しています。この論文では、一般的な量販ジャマーの代表的なケースとしてシミュレートされた 3 つの妨害干渉の存在下で、GNSS ソフトウェアスナップショットレシーバーアーキテクチャの文脈で RIM 手法を評価します。GNSS スナップショット受信機における信号の量子化の効果について、干渉緩和を中心に研究しています。結果は、量子化ダイナミックレンジが有限であることに起因するクリッピング効果が信号歪みを引き起こし、量子化ビット数が少ない場合には望ましくない受信機性能につながることを示唆しています。しかし、RIM を適用すると、可視衛星ビークルの数、位置・速度・時間（PVT）解の利用可能性、および観測された搬送波対雑音密度比の点で、量子化ビット数に比例した利得が観測されます。

第 36 回航法研究所衛星部門国際技術会議（ION GNSS+ 2023）の議事録 2023 年
9 月 11 ～ 15 日
ハイアット リージェンシー デンバー
コロラド州デンバー

Testing a Coherent Software Defined Radio Platform for Detection of Angle of Arrival of RF Signals

Lucca Trapani, Fred Taylor, Evan Gattis, Yh Chen, Sherman Lo, Todd, Walter, Dennis Akos

Peer Reviewed

Abstract: Past efforts in characterizing and preventing GPS/GNSS signal multipath propagation and interference have led to the development of commercial-off-the shelf (COTS) advanced receiver platforms capable of making angle-of-arrival (AoA) measurements. This paper investigates the testing of a low-cost, coherent radio platform called the KrakenSDR. The KrakenSDR is an experimental platform which has only recently become available and has a wide range of RF applications. In this work the KrakenSDR receiver functionality is characterized to better understand how it operates. Key components of the KrakenSDR such as the phase calibration, antenna array, and signal processing in a multiple signal classification (MUSIC) algorithm are studied. Laboratory testing with a function generator verified that the KrakenSDR can achieve phase coherence across its five input channels. In the field AoA testing was performed with a continuous wave (CW) RF signal source at 900 MHz. This testing revealed that the KrakenSDR can make AoA measurements to an accuracy within its specified field of resolution and also produces a confidence metric which can be used to check the accuracy of measurements. The KrakenSDR has a frequency range of 24 MHz – 1766 MHz making it capable of working at GNSS frequencies. However, there has not been an opportunity to test the KrakenSDR in the GNSS band yet. The future goal of this research is to extend the KrakenSDR into the GNSS range and further characterize its performance, ideally to be used in a GPS/GNSS interference localization system.

Published in: Proceedings of the 36th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2023)
September 11 - 15, 2023
Hyatt Regency Denver
Denver, Colorado

RF 信号の到来角度を検出するためのコヒーレント ソフトウェア無線プラットフォームのテスト

ルッカ・トラパーニ、フレッド・テイラー、エヴァン・ガティス、ヤー・チェン、シャーマン・ロー、トッド、ウォルター、デニス・エイコス

GPS/GNSS 信号のマルチパス伝播と干渉を特徴づけ、防止するというこれまでの取り組みにより、到来角（AoA）測定が可能な市販の（COTS）高度な受信機プラットフォームの開発につながりました。この論文では、KrakenSDR と呼ばれる低コストのコヒーレント無線プラットフォームのテストについて調査します。KrakenSDR は、最近になって利用可能になった実験的なプラットフォームであり、幅広い RF アプリケーションを備えています。この作業では、KrakenSDR 受信機の機能がどのように動作するかをよりよく理解できるように特徴付けられています。位相校正、アンテナ アレイ、多重信号分類（MUSIC）アルゴリズムでの信号処理など、KrakenSDR の主要コンポーネントが研究されています。ファンクションジェネレーターを使用した実験室テストでは、KrakenSDR が 5 つの入力チャンネル全体で位相コヒーレンスを達成できることが確認されました。現場では、900 MHz の連続波（CW）RF 信号源を使用して AoA テストが実行されました。このテストにより、KrakenSDR は、指定された分解能フィールド内の精度で AoA 測定を行うことができ、測定の精度をチェックするために使用できる信頼性メトリックも生成できることが明らかになりました。KrakenSDR は 24 MHz ～ 1766 MHz の周波数範囲を備えており、GNSS 周波数で動作できます。ただし、GNSS 帯域で KrakenSDR をテストする機会はまだありません。この研究の将来の目標は、KrakenSDR を GNSS 範囲に拡張し、その性能をさらに特徴づけ、理想的には GPS/GNSS 干渉位置特定システムで使用することです。

第 36 回航法研究所衛星部門国際技術会議（ION GNSS+ 2023）の議事録 2023 年
9 月 11 ～ 15 日
ハイアット リージェンシー デンバー
コロラド州デンバー

Wiener Disorder Detection Method for Anti-Spoofing in GNSS Navigation Kalman Filters

Steven E. Langel, John David Quartararo, Joseph Cisneros, Kevin Greco

Abstract: This paper describes the adaptation of an algorithm, originally designed to detect a ramp deviation in a Wiener process, to spoofing detection in global navigation satellite system (GNSS, e.g., GPS) receivers. Imperfectly compensated spoofing signals exhibit common-mode errors across all signals broadcast by a single transmitter, driven by inaccurate compensation of the spoofer-to-receiver transmission channel (range and range rate). Those common-mode delay and frequency errors can affect the clock bias and frequency estimates that the victim receiver calculates to estimate its position, velocity, and time (PVT). In a benign situation (i.e., no spoofing), the change in clock bias and frequency drift over time is determined primarily by the receiver's oscillator. Given that frequency drift is typically modeled as a Wiener process, our hypothesis was that the algorithm in [1] could be adapted to detect spoofer-induced deviations of clock frequency drift from the nominally expected stochastic behavior. First, the Wiener process ramp deviation algorithm is reviewed and then its application to spoofing detection in GNSS Kalman filters is discussed and formulated. Several practical issues are addressed, such as finite memory, computer processing limitations, and efficient approaches to reduce redundant calculations. Monte Carlo simulations characterizing false alarm and spoofing detection performance are presented. Finally, conclusions and recommendations for future work are presented.

Published in: Proceedings of the 34th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2021)
September 20 - 24, 2021
Union Station Hotel
St. Louis, Missouri

GNSS ナビゲーション カルマン フィルターにおけるなりすまし防止のためのウィーナー障害検出方法

スティーヴン・E・ランゲル、ジョン・デヴィッド・クアルタラロ、ジョセフ・シスネロス、ケビン・グレコ

この論文では、もともとウィーナー過程におけるランプ偏差を検出するために設計されたアルゴリズムを、全地球航法衛星システム（GNSS、たとえば GPS）受信機におけるスプーフィング検出に適用する方法について説明します。不完全に補償されたスプーフィング信号は、スプーファーから受信機への伝送チャネル（距離と距離レート）の不正確な補償によって引き起こされ、単一の送信機によってブロードキャストされるすべての信号にわたってコモンモード エラーを示します。これらのコモンモード遅延と周波数誤差は、被害受信機が位置、速度、時間（PVT）を推定するために計算するクロック バイアスと周波数推定に影響を与える可能性があります。問題のない状況（つまり、スプーフィングがない）では、時間の経過に伴うクロック バイアスと周波数ドリフトの変化は、主に受信機の発振器によって決まります。周波数ドリフトが一般にウィーナー過程としてモデル化されることを考慮すると、[1] のアルゴリズムを適応させて、スプーファーによって引き起こされるクロック周波数ドリフトの、名目上予想される確率的動作からの偏差を検出できるのではないかという仮説が立てられました。まず、ウィーナー プロセス ランプ偏差アルゴリズムをレビューし、次に GNSS カルマン フィルターでのスプーフィング検出へのその適用について議論し、定式化します。有限のメモリ、コンピュータ処理の制限、冗長な計算を削減するための効率的なアプローチなど、いくつかの実際的な問題に対処します。誤警報とスプーフィング検出パフォーマンスを特徴付けるモンテカルロ シミュレーションが表示されます。最後に、結論と今後の研究への推奨事項を示します。

補足説明:
ウィーナープロセス（Wiener process）は、確率論と統計学の分野で使われる連続時間確率過程の一つです。これは、ブラウン運動（Brownian motion）とも呼ばれます。ウィーナープロセスは、時刻が連続的であり、各時刻における変化が確率的で独立している性質を持っています。ウィーナープロセスは、金融工学、物理学、統計学、制御工学などのさまざまな分野で使用されます。金融の文脈では、ウィーナープロセスは株価のモデリングなどで応用され、統計学では確率過程の基本的な例として扱われます。また、制御工学ではブラウン運動の性質を利用してシステムのノイズをモデリングするために使われることもあります。

第 34 回航法研究所衛星部門国際技術会議（ION GNSS+ 2021）の議事録 2021 年
9 月 20 ～ 24 日ミズーリ州
セントルイス ユニオン ステーション ホテル

GNSS Anti-Spoofing Defense Based on Cooperative Positioning

Akmal Rustamov, Neil Gogoi, Alex Minetto and Fabio Dovis

Peer Reviewed

Abstract: Radio navigation is of utmost importance in several application fields. Nowadays, many civil and professional applications massively rely on the Global Navigation Satellite System (GNSS) and related technologies to accurately estimate position and time. Existing GNSS-based systems are threatened by malicious attacks among which spoofing and meaconing constitute severe challenges to the receiver. Several of such GNSS systems constitute mass market applications and devices, and a threat to the GNSS receiver could have cascading effects at application levels and for interconnected systems. Networked GNSS receivers are in general ubiquitous because any receiver embedded in a complex system such as a smart device or smart connected cars can exploit network connectivity. This novel generation of valuable-performance GNSS receivers are prone both to standard RF spoofing attacks and to cyber-attacks conceived to hijack complex network based services such as DGNSS-based cooperative positioning. By means of a set of experimental tests, this paper highlights possible metrics to be checked to identify malicious attacks to the positioning and navigation systems in mass market connected devices. The network-based exchange of GNSS data such as GNSS raw measurements recently disclosed in Android smart devices is conceived in this work to offer the possibility to compare or combine such metrics to better identifies spoofing and meaconing attacks.

Published in: Proceedings of the 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2020)
September 21 - 25, 2020

協調測位に基づく GNSS アンチスプーフィング防御

アクマル・ルスタモフ、ニール・ゴゴイ、アレックス・ミネット、ファビオ・ドーヴィス

無線ナビゲーションは、いくつかの応用分野で最も重要です。現在、多くの民間および専門的アプリケーションは、位置と時刻を正確に推定するために全地球航法衛星システム（GNSS）および関連テクノロジーに大きく依存しています。既存の GNSS ベースのシステムは悪意のある攻撃の脅威にさらされており、その中にはスプーフィングやミーコンが受信機にとって深刻な課題となります。このような GNSS システムのいくつかは大衆市場のアプリケーションやデバイスを構成しており、GNSS 受信機に対する脅威はアプリケーション レベルや相互接続されたシステムに連鎖的な影響を与える可能性があります。スマート デバイスやスマート コネクテッド カーなどの複雑なシステムに組み込まれた受信機はネットワーク接続を活用できるため、ネットワーク接続された GNSS 受信機は一般にユビキタスです。この新世代の貴重なパフォーマンスの GNSS 受信機は、標準的な RF スプーフィング攻撃と、DGNSS ベースの協調測位などの複雑なネットワーク ベースのサービスをハイジャックすることを目的としたサイバー攻撃の両方の影響を受けやすいです。このペーパーでは、一連の実験的テストを通じて、大衆向け接続デバイスの測位およびナビゲーション システムに対する悪意のある攻撃を特定するためにチェックすべき可能性のあるメトリクスに焦点を当てています。Android スマート デバイスで最近明らかにされた GNSS 生測定値などの GNSS データのネットワークベースの交換は、この研究で、そのようなメトリクスを比較または組み合わせて、スプーフィング攻撃やミーコン攻撃をより適切に識別する可能性を提供することを目的としています。

第 33 回航法研究所衛星部門国際技術会議（ION GNSS+ 2020）議事録
2020 年 9 月 21 ～ 25 日

GNSS Anti-Spoofing for a Multi-Element Antenna Array

Michael C. Esswein and Mark L. Psiaki

Abstract: New optimization-based methods are developed to use measured Direction-of-Arrival (DoA) information in order classify received GNSS signals into authentic and spoofed sets. These methods are designed for a resilient GNSS system that is being developed to mitigate GNSS spoofing and jamming by using signals from a small antenna array which consists of a set of patch antennas arranged in a “bug-eye” shape. The spoofing classification method of the present paper operates on the DoA outputs of the various signals’ trackers. The new method also uses the trackers’ computed estimation error covariances for their DoA estimates. The contribution of this paper is a multi-hypothesis test that considers all possible hypotheses about the authentic and spoofed sets of tracked signals. A combinatorial analysis is performed in order to generate all possible authentic-set/spoofed-set classifications for the given set of tracked signals and determine the correct authentic set among the different combinations. Results from Monte Carlo runs show that using DoA methods is suitable for determining the correct combinations, assuming there is large direction separation between the authentic GNSS signals and the spoofed signals. However, when using DoA and pseudorange techniques one can determine the correct combination regardless of the direction separations. Results also indicated that the assumptions made during the paper can be relaxed in order to successfully handle other scenarios, such as multiple directional spoofers.

Published in: Proceedings of the 32nd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2019)
September 16 - 20, 2019
Hyatt Regency Miami
Miami, Florida

複数素子アンテナ アレイの GNSS アンチスプーフィング

マイケル・C・エスワインとマーク・L・プシアキ

受信した GNSS 信号を本物のセットとスプーフィングされたセットに分類するために、測定された到着方向（DoA）情報を使用する新しい最適化ベースの方法が開発されました。これらの方法は、「バグアイ」形状に配置されたパッチ アンテナのセットで構成される小型アンテナ アレイからの信号を使用することにより、GNSS スプーフィングと妨害を軽減するために開発されている、回復力のある GNSS システム用に設計されています。本論文のスプーフィング分類方法は、さまざまな信号のトラッカーの DoA 出力に作用します。新しい方法では、トラッカーが計算した推定誤差の共分散を DoA 推定値に使用します。この論文の貢献は、追跡された信号の本物のセットと偽装されたセットに関するすべての可能な仮説を考慮する多重仮説テストです。組み合わせ分析は、追跡信号の特定のセットに対して考えられるすべての本物のセット/スプーフィング セットの分類を生成し、さまざまな組み合わせの中から正しい本物のセットを決定するために実行されます。モンテカルロ実行の結果は、本物の GNSS 信号とスプーフィングされた信号の間に大きな方向の分離があると仮定して、正しい組み合わせを決定するには DoA メソッドの使用が適していることを示しています。ただし、DoA および擬似距離技術を使用すると、方向の分離に関係なく正しい組み合わせを決定できます。結果はまた、多方向スプーファーなどの他のシナリオをうまく処理するために、論文中に立てられた仮定を緩和できることも示しました。

The 32nd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2019)
2019 年 9 月 16 ～ 20 日
ハイアット リージェンシー
マイアミ フロリダ州マイアミ

Android Raw GNSS Measurements as the New Anti-Spoofing and Anti-Jamming Solution

Damian Miralles, Nathan Levigne, Dennis M. Akos, Juan Blanch, and Sherman Lo

Abstract: Reliable radio navigation signals are of extreme importance. Nowadays we rely on Global Navigation Satellite System (GNSS) related technologies for a range of uses ranging from agricultural, financial, transportation and military applications. As such, providing existing systems with the tools to combat the threat presented by malicious spoofing or jamming attacks is critical. The paper explores the properties of the different sensors available on a smartphones and evaluates their potential for spoofing and jamming detection. By properly assessing key sensor properties, this work will detect spoofing or jamming by monitoring alarm triggers set by a combination of sensors including but not limited to: (1) network location provider, (2) combined Automatic Gain Control (AGC) and C/N0 engine, (3) inertial sensor data, and (4) pseudorange residual metrics. In addition, we investigate the existence of the solution on the smartphone and further discuss the sensors with potential in the identification if any type of interference attack. Combining all together is GNSSAlarm, an Android application (still under development) that creates a tool, based on resources already in the pocket of millions of individuals and develops an effective anti-spoofing, anti-jamming tool that will allow proper functionality when in the presence of spoofing attacks and will notify the user when under jamming attacks.

Published in: Proceedings of the 31st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2018)
September 24 - 28, 2018
Hyatt Regency Miami
Miami, Florida

新しいアンチスプーフィングおよびアンチジャミング ソリューションとしての Android Raw GNSS 測定

ダミアン ミラレス、ネイサン レヴィーン、デニス M. アコス、フアン ブランチ、シャーマン ロー

信頼性の高い無線ナビゲーション信号は非常に重要です。現在、私たちは農業、金融、輸送、軍事用途に至るまで、幅広い用途で全球測位衛星システム（GNSS）関連テクノロジーに依存しています。そのため、悪意のあるスプーフィング攻撃やジャミング攻撃によってもたらされる脅威に対抗するツールを既存のシステムに提供することが重要です。この論文では、スマートフォンで利用可能なさまざまなセンサーの特性を調査し、それらのスプーフィングおよび妨害検知の可能性を評価します。この取り組みでは、主要なセンサーの特性を適切に評価することにより、(1) ネットワーク ロケーション プロバイダー、(2) 自動利得制御（AGC）と C/ N0 エンジン、(3) 慣性センサー データ、および (4) 擬似距離残差メトリクス。さらに、スマートフォン上のソリューションの存在を調査し、あらゆるタイプの干渉攻撃を識別する可能性のあるセンサーについてさらに議論します。これらすべてを組み合わせたものが、GNSS Alarm という Android アプリケーション（まだ開発中）です。このアプリケーションは、すでに何百万人もの個人のポケットにあるリソースに基づいてツールを作成し、有効なスプーフィング対策、妨害対策ツールを開発します。スプーフィング攻撃の存在を検出し、ジャミング攻撃を受けている場合にはユーザーに通知します。

第 31 回航法研究所衛星部門国際技術会議（ION GNSS+ 2018）の議事録 2018 年
9 月 24 ～ 28 日
ハイアット リージェンシー マイアミ
フロリダ州マイアミ

Doppler Considerations and Phase Manifold Effects for Anti-jam Electronics

Adam Simmons, Russell Powell, Greg Reynolds, Laura McCrain, Timothy Pitt, Caleb Perry, Brian Baeder

Abstract: Due to the widespread use of anti-jam electronics (AJ-E) with controllable radiation pattern antennas (CRPA) in estimating direction of arrival (DOA), considerations of Doppler and contributions through antenna phase manifold should be considered for both error characterization in AJ-E covariance output and effectiveness of nulling algorithms. By considering the manifold effects, an observability space can be estimated a priori and provided to down-stream DOA filters. The observability space also provides an expected error characterization for AJ-E's signal covariance matrix used to derive weights for their individual antenna element feeds and taps. This estimated covariance matrix is typically derived from a windowed set of In-phase and Quadrature phase (IQ) samples collected over a set length of time (typically 1 ms). Most per-element delays are constant over this time period, but some vehicles hosting the AJ-E have roll rates which, when mapped through the antenna phase manifold, can create Doppler coloring of the covariance estimate. Even with benign roll rates, the manifold coloring of the Doppler can be significant. This paper examines the Doppler influence through a commercial CRPA's phase manifold and maps the per-component phase error perceived. The paper demonstrates the effect through software simulated IQ data samples and a commercial phase manifold.

Published in: 2018 IEEE/ION Position, Location and Navigation Symposium (PLANS)
April 23 - 26, 2018
Hyatt Regency Hotel
Monterey, CA

アンチジャムエレクトロニクスにおけるドップラーの考慮事項と位相多様体の効果

アダム・シモンズ、ラッセル・パウエル、グレッグ・レイノルズ、ローラ・マクレーン、ティモシー・ピット、ケイレブ・ペリー、ブライアン・ベイダー

到来方向（DOA）の推定において制御可能な放射パターン アンテナ（CRPA）を備えたアンチジャム エレクトロニクス（AJ-E）が広く使用されているため、AJ の両方のエラー特性評価では、ドップラーとアンテナ位相マニホールドによる寄与を考慮する必要があります。 -E 共分散出力とヌル化アルゴリズムの有効性。多様体効果を考慮することにより、可観測空間を先験的に推定し、下流の DOA フィルターに提供することができます。可観測性空間は、個々のアンテナ要素のフィードとタップの重みを導出するために使用される AJ-E の信号共分散行列の予想誤差特性評価も提供します。この推定共分散行列は通常、設定された時間長（通常 1 ミリ秒）にわたって収集された同相および直交位相（IQ）サンプルのウィンドウ化されたセットから導出されます。ほとんどの要素ごとの遅延はこの期間にわたって一定ですが、AJ-E をホストする一部の車両にはロール レートがあり、アンテナ位相マニホールドを通じてマッピングされると、共分散推定のドップラー カラーリングが発生する可能性があります。ロール レートが良好であっても、ドップラーの多様なカラーリングが顕著になる場合があります。この論文では、市販の CRPA の位相マニホールドを介してドップラーの影響を調査し、知覚されるコンポーネントごとの位相誤差をマッピングします。この論文では、ソフトウェアでシミュレートされた IQ データ サンプルと商用位相マニホールドを通じてその効果を実証しています。

2018 IEEE/ION Position, Location and Navigation Symposium（PLANS）
2018 年 4 月 23 ～ 26 日
ハイアット リージェンシー ホテル
モントレー、カリフォルニア州

Advantages of a Robust Multi-Antenna GNSS Receiver in UAV Flight Jamming Scenarios

Philipp Rudnik, Lothar Kurz, Andreas Winterstein, Manuel Cuntz

Abstract: The multi-antenna Global Navigation Satellite System (GNSS) receiver GALileo ANTenna (GALANT) has been developed at German Aerospace Center (DLR) since several years. Recently, effort has been spent to miniaturize the antennas and digital processing system in order to enable applications in the field of Unmanned Aerial Vehicle (UAV) navigation for example. In addition, array processing technologies have been further improved for this kind of application. This publication focuses on the conduction of flight test of the complete system and the therein occurring advantages towards a commercial receiver in difficult navigation scenarios like under the influence of jamming. The flight experiments are divided into two parts. Firstly, it is investigated how the different receivers react to corresponding jamming from the ground while the receiver is not moving, but is hovering close to the ground. During this experiment, the jamming power is increased step by step. The reference receiver goes into saturation, gradually loses all satellites, the position accuracy drops and finally no valid Position/Velocity/Timing (PVT) can be computed. In contrast, the GALANT receiver detects the interference and suppresses it appropriately based on spatial signal processing techniques. In the second part of the experiments, it is investigated how jamming signals emitted from ground affect the receiver during real flight scenarios. A static and directional jammer is set up and the UAV flies a trajectory passing multiple times through the beam. Interestingly the reference receiver does not only lose all satellites in track, like expected from the first experiment, but computes a false position increasingly diverging from ground truth before and after the total loss. The deviation of position is in the range of multiple hundred meters. The GALANT receiver is able to keep most of the satellites in track, and computes a continuous position with negligible deviation. The flight experiments conducted show that it is reasonable to protect UAVs appropriately against interference such as jamming. The tests also show that techniques, such as those presented, can be an effective solution to the stated problems. The developed robust, multi-antenna receiver outperformed the corresponding comparison receiver in the presented areas.

Published in: Proceedings of the 36th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2023)
September 11 - 15, 2023
Hyatt Regency Denver
Denver, Colorado

UAV 飛行妨害シナリオにおける堅牢なマルチアンテナ GNSS 受信機の利点

フィリップ・ルドニク、ローター・クルツ、アンドレアス・ヴィンターシュタイン、マヌエル・クンツ

マルチアンテナ全地球航法衛星システム（GNSS）受信機 GALileo ANTenna（GALANT）は、ドイツ航空宇宙センター（DLR）で数年にわたって開発されてきました。最近では、例えば無人航空機（UAV）ナビゲーションの分野での応用を可能にするために、アンテナとデジタル処理システムの小型化に努力が払われています。さらに、この種のアプリケーション向けにアレイ処理技術がさらに改良されました。この出版物は、完全なシステムの飛行テストの実施と、妨害電波の影響下などの困難な航行シナリオにおいて商用受信機に対して生じる利点に焦点を当てています。飛行実験は 2 つのパートに分かれています。まず、受信機が移動していないが地面の近くでホバリングしているときに、さまざまな受信機が対応する地上からの妨害にどのように反応するかを調査します。この実験では、妨害電力を段階的に増加させます。基準受信機は飽和状態になり、徐々にすべての衛星を失い、位置精度が低下し、最終的には有効な位置/速度/タイミング（PVT）を計算できなくなります。対照的に、GALANT 受信機は干渉を検出し、空間信号処理技術に基づいて適切に抑制します。実験の第 2 部では、実際の飛行シナリオ中に地上から発せられる妨害信号が受信機にどのような影響を与えるかを調査します。静的で指向性のあるジャマーがセットアップされ、UAV はビームを複数回通過する軌道を飛行します。興味深いことに、最初の実験で予想されたように、基準受信機は軌道上のすべての衛星を失うだけでなく、完全な損失の前後で地上の真実からますます乖離する誤った位置を計算します。位置のずれは数百メートルの範囲にあります。GALANT 受信機は、ほとんどの衛星を軌道上に維持することができ、偏差を無視して連続的な位置を計算します。実施された飛行実験は、妨害などの干渉から UAV を適切に保護することが合理的であることを示しています。このテストでは、ここで紹介したような手法が、前述の問題に対する効果的な解決策となり得ることも示しています。開発された堅牢なマルチアンテナ受信機は、提示された領域で対応する比較受信機を上回りました。

第 36 回航法研究所衛星部門国際技術会議（ION GNSS+ 2023）の議事録 2023 年
9 月 11 ～ 15 日
ハイアット リージェンシー デンバー
コロラド州デンバー

Variation Analysis of Satellite Navigation Message and its Application to Anti-spoofing

Jianfeng Li, Hong Li, Fei Wang, Hang Ruan, ZhongXiao Wang, and Mingquan Lu

Peer Reviewed

Abstract: Global Navigation Satellite System (GNSS) is widely applied to our daily life with its stable service. The GNSS control segment routinely generates navigation message based on a prediction model and the measurements from global monitor stations. Navigation message includes each satellite's clock correction, ephemeris, and almanac, which are stable and change by certain rules. The paper analyzes these parameters of Global Positioning System (GPS) and BeiDou System (BDS). Based on different changing rules of parameters, the paper divides all parameters into four categories and briefly discusses their applications in anomaly detection and anti-spoofing. Further, the computed satellite position deviations by ephemerides and almanacs of different time are researched and relevant mathematical model is established. Also, the computed clock deviations are discussed. With the increasing use of GNSS, its vulnerability has caused much concern. In general, there are many spoofing methods. In order to deceive a victim receiver to a predetermined position or time, some spoofers may change navigation message. The above analysis results can be applied to check such spoofing attacks. So two threshold models are established and their advantages and disadvantages are discussed. Combining two threshold models, the paper proposes a method to effectively utilize navigation message for anti-spoofing. Finally, the method is implemented on GPS/BDS receivers and the relevant experimental results show that it is feasible and effective in different deception scenarios where navigation message is tampered.

Published in: Proceedings of the 2018 International Technical Meeting of The Institute of Navigation
January 29 - 1, 2018
Hyatt Regency Reston
Reston, Virginia

衛星航法メッセージの変動解析となりすまし対策への応用

李建峰、李宏、王飛、阮杭、王忠孝、盧明泉

全地球測位衛星システム（GNSS）は、安定したサービスを提供し、私たちの日常生活に広く応用されています。GNSS 制御セグメントは、予測モデルとグローバル監視ステーションからの測定値に基づいてナビゲーション メッセージを定期的に生成します。航法メッセージには、各衛星の時計補正、軌道暦、アルマナックが含まれており、これらは安定していて特定の規則によって変化します。この論文では、全地球測位システム（GPS）と北斗システム（BDS）のこれらのパラメーターを分析します。この論文では、パラメータのさまざまな変更ルールに基づいて、すべてのパラメータを 4 パラメータに分類し、異常検出とスプーフィング対策におけるそれらのアプリケーションについて簡単に説明します。さらに、異なる時刻のエフェメリドとアルマナックによって計算された衛星位置偏差が研究され、関連する数学的モデルが確立されます。また、計算されたクロック偏差についても説明します。GNSS の使用が増えるにつれて、その脆弱性が大きな懸念を引き起こしています。一般に、なりすましの手法は数多くあります。被害者の受信機をだまして所定の位置または時刻に移動させるために、一部のなりすまし者はナビゲーション メッセージを変更する場合があります。上記の分析結果は、このようななりすまし攻撃のチェックに適用できます。そこで 2 つの閾値モデルを確立し、その利点と欠点について説明します。この論文では、2 つのしきい値モデルを組み合わせて、スプーフィング対策にナビゲーション メッセージを効果的に利用する方法を提案しています。最後に、この方法は GPS/BDS 受信機に実装されており、関連する実験結果は、ナビゲーション メッセージが改ざんされるさまざまな欺瞞シナリオにおいて、この方法が実行可能かつ効果的であることを示しています。

航海学会の 2018 年国際技術会議議事録 2018
年 1 月 29 ～ 1 日
ハイアット リージェンシー レストン
バージニア州レストン

Authentication by Polarization: A Powerful Anti-Spoofing Method

Wim De Wilde, Jean-Marie Sleewaegen, Bruno Bougard, Gert Cuypers, Alexander Popugaev, Markus Landmann, Christopher Schirmer, Daniel Egea Roca, José A. López-Salcedo, Gonzalo Seco Granados

Abstract: This paper presents a method to detect and mitigate a spoofing attack by means of a dual polarized antenna. It exploits the similarity in polarization of spoofed satellites to identify spoofed satellites and copes with three major challenges. A first challenge is to avoid false alarms, which could be triggered by occasional polarization alignment of authentic satellites. The second challenge is the detection of spoofed signals out of a mix of spoofed and non-spoofed signals, as is the case in most practical spoofing attacks. The final challenge is to be able to work with spoofed signals from RHCP spoofing antennas operating from a higher elevation. The technique was developed based on analysis of a large amount of experimental signal data recorded in spoofed and non-spoofed environments. The paper first describes the recording system, which uses a high-performance dual polarized antenna, optimized for low axial ratio. This connects to a multi-frequency multi-constellation receiver, supporting concurrent coherent tracking of the RHCP and LHCP signal components provided by the antenna. We subsequently discuss the measurement campaign. It is rather straightforward to collect data in a variety of non-spoofed environments to build a database of scenarios which are supposed to yield a negative spoofing indication. This doesn't hold for spoofing scenarios, because of regulatory constraints. Therefore, the spoofing tests were done in a special anechoic chamber which can simulate both polarization and angle of arrival of satellite signals. This wave field synthesis (WFS) testbed was configured to create a mix of satellite signals, some of them emulating authentic signals and the other ones representing the spoofer. The WFS testbed was used to simulate an advanced matched power timing attack. Finally, the paper discusses a new spoofing detection algorithm, based on the experimental data. We present an analysis of the spoofing classification performance, analyzing metrics for probability of false alarm and probability of detection.

Published in: Proceedings of the 31st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2018)
September 24 - 28, 2018
Hyatt Regency Miami
Miami, Florida

偏光による認証: 強力なスプーフィング防止方法

ヴィム・デ・ワイルド、ジャン＝マリー・スリーヴァーゲン、ブルーノ・ブーガード、他

この文書では、二重偏波アンテナを使用してスプーフィング攻撃を検出し、軽減する方法を紹介します。これは、なりすまし衛星の偏波の類似性を利用してなりすまし衛星を識別し、3 つの主要な課題に対処します。最初の課題は、本物の衛星の時折の偏波調整によって引き起こされる可能性がある誤警報を回避することです。2 番目の課題は、ほとんどの実際のスプーフィング攻撃の場合と同様に、スプーフィングされた信号とスプーフィングされていない信号が混在する中からスプーフィングされた信号を検出することです。最後の課題は、より高い標高から動作する RHCP スプーフィング アンテナからのスプーフィング信号を処理できるようにすることです。この技術は、スプーフィングされた環境およびスプーフィングされていない環境で記録された大量の実験信号データの分析に基づいて開発されました。この論文ではまず、低軸比に最適化された高性能二重偏波アンテナを使用する記録システムについて説明します。これは、多周波数マルチコンステレーション受信機に接続し、アンテナによって提供される RHCP および LHCP 信号成分の同時コヒーレント トラッキングをサポートします。続いて、測定キャンペーンについて説明します。さまざまな非スプーフィング環境でデータを収集して、否定的なスプーフィングの兆候を示すシナリオのデータベースを構築することはかなり簡単です。規制上の制約があるため、これはスプーフィングのシナリオには当てはまりません。したがって、なりすましテストは、衛星信号の偏波と到来角度の両方をシミュレートできる特別な電波暗室で行われました。この波面合成（WFS）テストベッドは、衛星信号の混合を作成するように構成されており、そのうちのいくつかは本物の信号をエミュレートし、他の信号はスプーファーを表します。WFS テストベッドは、高度なマッチング パワー タイミング攻撃をシミュレートするために使用されました。最後に、実験データに基づいて、新しいなりすまし検出アルゴリズムについて説明します。スプーフィング分類パフォーマンスの分析を示し、誤報の確率と検出の確率のメトリクスを分析します。

第 31 回航法研究所衛星部門国際技術会議（ION GNSS+ 2018）の議事録 2018 年
9 月 24 ～ 28 日
ハイアット リージェンシー マイアミ
フロリダ州マイアミ

Fault-Robust GPS Spoofing Mitigation with Expectation-Maximization

Ashwin Vivek Kanhere, Grace Gao

Abstract: The possibility of measurement faults and spoofing attacks poses real-world risks to accurate and safe localization using GPS measurements. Measurement faults introduce additive biases in individual measurements that might be inconsistent across measurements while spoofing attacks introduce consistent additive biases in all measurements. Both of these effects introduce errors in the localization solution estimated using these affected measurements. Recognizing these risks, researchers have developed solutions to mitigate these spoofing attacks and measurement faults, usually individually, by using redundant measurements or explicitly modelling and estimating the attack and fault magnitudes. When these localization methods model spoofing or faults individually, they can raise a large number of false spoofing alerts in the presence of faults or incorrectly incorporate spoofing attacks when accounting for faults. However, as both spoofing attacks and faulty measurements can be encountered in the real world, there is a need to mitigate both jointly when performing GPS localization. In this work, we propose an expectation-maximization (EM)-based method for jointly mitigating the effects of spoofing attacks and measurement faults during localization. During the expectation step, in a two-step process, we first estimate the likelihood that the GPS measurements are spoofed at a particular time instant using sensor level redundancy. We then estimate the likelihood that individual GPS measurements are faulty at that time instant using measurement-level redundancy. Finally, during the maximization step, both these likelihood estimates are combined to de-weigh GPS measurements that are used for localization. We also highlight a particular implementation of our proposed method. Our method estimates the likelihood of GPS spoofing using M-estimation and the likelihood of measurement faults along with state estimate with a factor graph optimization framework with switchable constraints (SC-FGO). We experimentally validate our proposed approach in simulations, comparing to three different baseline implementations, to show that our method successfully mitigates the effects of both spoofing and faulty measurements.

Published in: Proceedings of the 36th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2023)
September 11 - 15, 2023
Hyatt Regency Denver
Denver, Colorado

期待値の最大化による障害に強い GPS スプーフィングの軽減

アシュウィン・ヴィヴェク・カンヘレ、グレース・ガオ

測定エラーやなりすまし攻撃の可能性により、GPS 測定を使用した正確かつ安全な位置特定に対して現実世界のリスクが生じます。測定障害により、個々の測定値に加法的なバイアスが生じ、測定全体で一貫性がなくなる可能性がありますが、スプーフィング攻撃では、すべての測定値に一貫した加法的なバイアスが生じます。これらの影響はどちらも、影響を受ける測定値を使用して推定された位置推定ソリューションに誤差をもたらします。これらのリスクを認識して、研究者は、冗長な測定を使用するか、攻撃と障害の規模を明示的にモデル化して推定することにより、通常は個別に、これらのなりすまし攻撃と測定障害を軽減するソリューションを開発しました。これらのローカリゼーション方法がスプーフィングや障害を個別にモデル化すると、障害が存在する場合に大量の誤ったスプーフィング アラートが生成されたり、障害を説明するときに誤ってスプーフィング攻撃が組み込まれたりする可能性があります。ただし、現実世界ではスプーフィング攻撃と誤った測定の両方が発生する可能性があるため、GPS 位置特定を実行する際には両方を組み合わせて軽減する必要があります。この研究では、位置特定中のスプーフィング攻撃と測定障害の影響を共同で軽減するための期待値最大化（EM）ベースの方法を提案します。予想ステップでは、2 段階のプロセスで、まずセンサー レベルの冗長性を使用して、特定の時点で GPS 測定値が偽装される可能性を推定します。次に、測定レベルの冗長性を使用して、その時点での個々の GPS 測定が誤っている可能性を推定します。最後に、最大化ステップ中に、これらの尤度推定値の両方が組み合わされて、位置特定に使用される GPS 測定値の重みが軽減されます。また、提案した方法の特定の実装についても強調します。私たちの方法では、M 推定を使用して GPS スプーフィングの可能性を推定し、切り替え可能な制約を備えたファクター グラフ最適化フレームワーク（SC-FGO）による状態推定とともに測定エラーの可能性を推定します。提案したアプローチをシミュレーションで実験的に検証し、3 つの異なるベースライン実装と比較して、私たちの方法がスプーフィングと誤った測定の両方の影響を軽減できることを示します。

第 36 回航法研究所衛星部門国際技術会議（ION GNSS+ 2023）の議事録 2023 年
9 月 11 ～ 15 日
ハイアット リージェンシー デンバー
コロラド州デンバー

A GNSS Spoofing Detection Method Based on Raw GNSS/IMU/Camera Measurements

Xiao Zhou, Hong Li, Mingquan Lu

Abstract: Global navigation satellite system (GNSS) spoofing is an emerging threat to GNSS security while GNSS plays an important role in military and civilian fields. Recently, taking into account IMU's characteristics of no external dependence, as well as the low cost and high precision of cameras, graph optimization-based SLAM (Simultaneous Localization and Mapping) system that is coupled with GNSS measurements has been developed to achieve a more stable positioning performance. However, few existing GNSS spoofing detection methods can be directly adapted to this kind of system. According to our analysis, the residuals in graph optimization can reflect the consistency of different sensor measurements. We proposed a detector exploiting the pseudorange residuals in the graph optimization. After the initialization of coordinates, the proposed method can generate the detector based on raw GNSS/IMU/camera measurements. Experimental results in different GNSS spoofing scenarios have verified the detection performance of our method.

Published in: Proceedings of the 2023 International Technical Meeting of The Institute of Navigation
January 24 - 26, 2023
Hyatt Regency Long Beach
Long Beach, California

Pages: 377 - 384

Cite this article: Zhou, Xiao, Li, Hong, Lu, Mingquan, "A GNSS Spoofing Detection Method Based on Raw GNSS/IMU/Camera Measurements," *Proceedings of the 2023 International Technical Meeting of The Institute of Navigation*, Long Beach, California, January 2023, pp. 377-384.
https://doi.org/10.33012/2023.18631

生の GNSS/IMU/カメラ測定に基づく GNSS スプーフィング検出方法

シャオ・ジョウ、ホン・リー、ミンクアン・ルー

全地球航法衛星システム（GNSS）のなりすましは、GNSS セキュリティに対する新たな脅威となっていますが、GNSS は軍事および民間分野で重要な役割を果たしています。最近では、外部依存性がないという IMU の特性と、カメラの低コストおよび高精度を考慮して、より安定した画像を実現するために、GNSS 測定と組み合わせたグラフ最適化ベースの SLAM（Simultaneous Localization and Mapping）システムが開発されました。位置決め性能。ただし、この種のシステムに直接適用できる既存の GNSS スプーフィング検出方法はほとんどありません。私たちの分析によると、グラフ最適化の残差は、さまざまなセンサー測定の一貫性を反映している可能性があります。我々は、グラフ最適化において擬似距離残差を利用する検出器を提案した。座標の初期化後、提案された方法は生の GNSS/IMU/カメラ測定値に基づいて検出器を生成できます。さまざまな GNSS スプーフィング シナリオでの実験結果により、私たちの方法の検出パフォーマンスが検証されました。

航海学会の 2023 年国際技術会議の議事録 2023 年
1 月 24 ～ 26 日
ハイアット リージェンシー ロングビーチ
カリフォルニア州ロングビーチ

Smartphone Behaviour under Sophisticated Time Synchronized and Record and Replay Spoofing Attacks

Ronny Blum, Himanshu Sharma, Thomas Pany

Abstract: With more than 70 percent of the world population being the Smartphone user and 77 percent of the smartphone users still rely on the Smartphone positioning for navigation [1], there is no doubt that the Smartphones are amongst the largest Global Navigation Satellite System (GNSS) receiver installed device in the GNSS market, 90 percent of the GNSS receivers in the price segment of less than 5 € are used for smartphones and wearables, which is set to be almost 1.8 billion Smartphones by 2029 [2]. With such a high share in the GNSS market, the threat of GNSS spoofing is no longer limited to the critical infrastructure only. Till date GNSS chip inside the smartphone is a black box providing positioning solution with no access to the baseband processing technique. But, with the availability of GNSS raw measurements through Android API [3], the researcher get access to wide range of measurements, which not only are important for the development of improved positioning algorithms but can also be vital for integrity check. The vulnerability of smartphones to the spoofing attack and the usage of GNSS raw measurements to counter such attack has been presented in [4] [5]. But, with the availability of newer generation smartphone supporting dual frequency and multi-constellation, it is extremely important to analyze their behaviour under such attack. In this work it was tested if an additional L5 frequency protects against an GPS L1 and Galileo E1 attack. Other GNSS raw measurements like the Carrier to Noise ratio (C/N0) are also a good candidates to examine the influence of a spoofing attack. In this work we present the results of over the air smartphone spoofing experiments with a repeater in a shielded box. The experiment was conducted with the wide range of smartphones with different manufactures, Operating Systems and different GNSS chipsets to examine their behaviour under the attack. We tested the behaviour under two different types of spoofing, the Record and Replay attack and the more sophisticated approach of a time synchronized signal generator attack. Record and Replay is just the recording of a Global Navigation Satellite System (GNSS) file with a certain bandwidth and retransmitting the recorded file later on with a high power. Signal generator spoofing is the generation and emission of artificial authentic GNSS-signals with a signal generator, which tries to imitate the real satellite signals in terms of code phase, Doppler and navigation bit as good as possible to induce a wrong time and/or position output on the victim receiver. The artificial signals should have ideally a slightly higher amplitude at the target position than the authentic signals in order to get tracked from the receiver. We investigated synchronized attacks with a purchasable Jamming and Spoofing generator from [6], which is able to perform a synchronized spoofing attack to real satellite signals and by now Galileo E1B/C and GPS L1 C/A signals are generated from the spoofing device. Beside the position, the C/N0 was analyzed, which changed for all satellite signals when the spoofing attack started. This parameter was also analyzed for common receivers and proposed as anti-spoofing parameter in [7]. For the sophisticated attack, all smartphones could be spoofed, meaning the position could be shifted kilometres away from the starting position, which was also the case when the internet was set on in the smartphones. Some smartphones were also set to track L1 and L5 signals, but could still be spoofed, which was unexpected since the spoofing signal only included GPS L1 and Galileo E1 signals. The Record and Replay attack, which is relatively easy to perform and the equipment is also relatively cheap, lead in the most smartphones to a jamming behaviour, meaning that the authentic signals were just overpowered and the spoofing signals were not tracked. But still some could be spoofed as well. The analysis showed that even in the presence of A-GPS (Wi-Fi), it was possible to spoof the smartphones. Also the fact that the spoofer did not need to include L5 signals for a successful spoofing, showed the severe vulnerability against spoofing.

Published in: Proceedings of the 2022 International Technical Meeting of The Institute of Navigation
January 25 - 27, 2022
Hyatt Regency Long Beach
Long Beach, California

高度な時刻同期によるスマートフォンの挙動となりすまし攻撃の記録・再生

ロニー・ブラム、ヒマンシュ・シャルマ、トーマス・パニー

世界人口の 70% 以上がスマートフォン ユーザーであり、スマートフォン ユーザーの 77% が依然としてナビゲーションにスマートフォンの測位に依存している［1］ため、スマートフォンが最大規模の全地球航法衛星システム（GNSS）の 1 つであることは疑いの余地がありません。GNSS 市場における受信機搭載デバイスの中で、5 ユーロ未満の価格帯の GNSS 受信機の 90% はスマートフォンとウェアラブルに使用されており、2029 年までにスマートフォンが約 18 億台になると見込まれています［2］。GNSS 市場での高いシェアにより、GNSS スプーフィングの脅威は重要なインフラストラクチャのみに限定されなくなりました。これまで、スマートフォン内の GNSS チップは、ベースバンド処理技術にアクセスできない測位ソリューションを提供するブラック ボックスでした。しかし、Android API［3］を通じて GNSS の生の測定値が利用できるようになったことで、研究者は広範囲の測定値にアクセスできるようになり、これは改良された測位アルゴリズムの開発にとって重要であるだけでなく、整合性チェックにとっても不可欠となり得ます。スプーフィング攻撃に対するスマートフォンの脆弱性と、そのような攻撃に対抗するための GNSS 生の測定値の使用については、［4］［5］で説明されています。しかし、デュアル周波数とマルチコンステレーションをサポートする新世代のスマートフォンが利用可能になったことにより、このような攻撃下での動作を分析することが非常に重要になります。この研究では、追加の L5 周波数が GPS L1 および Galileo E1 攻撃から保護されるかどうかがテストされました。搬送波対雑音比（C/N0）などの他の GNSS の生の測定値も、スプーフィング攻撃の影響を調べるのに適した候補です。この研究では、シールド ボックス内の中継器を使用した無線スマートフォンのなりすまし実験の結果を紹介します。この実験は、攻撃時の動作を調べるために、さまざまなメーカー、オペレーティング システム、さまざまな GNSS チップセットを備えた幅広いスマートフォンで実施されました。私たちは、記録再生攻撃と、より高度な時間同期信号発生器攻撃という 2 つの異なるタイプのスプーフィングの下で動作をテストしました。記録と再生は、特定の帯域幅で全地球航法衛星システム（GNSS）ファイルを記録し、記録されたファイルを後で高出力で再送信することです。信号発生器のスプーフィングとは、信号発生器を使用して人工的に本物の GNSS 信号を生成および送信することです。信号発生器は、コード位相、ドップラー、ナビゲーション ビットの点で実際の衛星信号を可能な限り模倣して、間違った時間や位置を誘導しようとします。被害者受信機の出力。受信機から追跡できるように、人工信号は理想的には、ターゲット位置で本物の信号よりわずかに高い振幅を持つ必要があります。［6］から購入可能なジャミングおよびスプーフィング ジェネレーターを使用した同期攻撃を調査しました。これは、実際の衛星信号に対して同期スプーフィング攻撃を実行することができ、現在では、Galileo E1B/C および GPS L1 C/A 信号がスプーフィング デバイスから生成されています。位置に加えて、C/N0 も分析されました。これは、スプーフィング攻撃が開始されたときにすべての衛星信号に対して変化しました。このパラメータは一般的な受信機についても分析され、［7］でスプーフィング対策パラメータとして提案されました。高度な攻撃では、すべてのスマートフォンがなりすましされる可能性があります。つまり、位置が開始位置から数キロ離れたところに移動する可能性があります。これは、スマートフォンでインターネットがオンに設定されている場合にも当てはまります。一部のスマートフォンは L1 および L5 信号を追跡するように設定されていましたが、それでもスプーフィングされる可能性がありました。スプーフィング信号には GPS L1 信号と Galileo E1 信号のみが含まれていたため、これは予想外でした。記録再生攻撃は実行が比較的簡単で、機器も比較的安価ですが、ほとんどのスマートフォンで妨害行為を引き起こします。これは、本物の信号が強力すぎるだけで、なりすまし信号が追跡されないことを意味します。しかし、それでも一部はなりすましの可能性もあります。分析の結果、A-GPS（Wi-Fi）が存在する場合でもスマートフォンになりすますことが可能であることがわかりました。また、スプーファーがスプーフィングを成功させるために L5 信号を含める必要がないという事実は、スプーフィングに対する深刻な脆弱性を示しています。

航海学会 2022 年国際技術会議議事録 2022 年 1 月 25 ～ 27 日
ハイアット リージェンシー ロングビーチ

GNSS Spoofing Detection Using Visual Inertial Odometry

Xiao Zhou, Hong Li, Jian Wen, Yimin Wei, Chun Yang, Mingquan Lu

Peer Reviewed

Abstract: Global navigation satellite system (GNSS) spoofing is becoming an emerging threat to GNSS security for it can induce fake positions at the victim receiver. Recently SLAM (Simultaneous Localization and Mapping) system that is coupled with GNSS has been developed to achieve a better positioning accuracy. However, few existing studies investigated the potential of such scheme to detect GNSS spoofing attacks. This paper proposes a spoofing detection method based on an open-source SLAM system, VINS (Visual-Inertial Navigation System)-Fusion. The proposed method starts with checking the displacement of GNSS measurements and multi-sensor estimation. After the check, the proposed method exploits the transformation matrix of the local frame in VINS-Fusion and the global frame, which is got from the pose-graph optimization. Considering that the transformation matrix is changing slowly generally after every optimization, the sudden change of the matrix may indicate the occurrence of spoofing attacks. We test the performance of VINS-Fusion to verify the necessity to implement spoofing detection in a vision-based state estimation system and explore whether VINS-Fusion can be used to detect spoofing. Moreover, experimental results over public datasets show the effectiveness of our spoofing detection method in certain spoofing scenarios with an acceptable false alarm probability and missed detection probability.

Published in: Proceedings of the 2022 International Technical Meeting of The Institute of Navigation
January 25 - 27, 2022
Hyatt Regency Long Beach
Long Beach, California

Pages: 1392 - 1404

Cite this article: Zhou, Xiao, Li, Hong, Wen, Jian, Wei, Yimin, Yang, Chun, Lu, Mingquan, "GNSS Spoofing Detection Using Visual Inertial Odometry," *Proceedings of the 2022 International Technical Meeting of The Institute of Navigation*, Long Beach, California, January 2022, pp. 1392-1404.
https://doi.org/10.33012/2022.18186

視覚慣性オドメトリを使用した GNSS スプーフィング検出

シャオ・ジョウ、ホン・リー、ジャン・ウェン、イーミン・ウェイ、チュン・ヤン、ミンクアン・ルー

全地球測位衛星システム（GNSS）のスプーフィングは、被害者の受信機に偽の位置を誘導する可能性があるため、GNSS セキュリティに対する新たな脅威となっています。最近、より優れた測位精度を達成するために、GNSS と組み合わせた SLAM（Simultaneous Localization and Mapping）システムが開発されました。しかし、GNSS スプーフィング攻撃を検出するためのこのようなスキームの可能性を調査した既存の研究はほとんどありません。本稿では、オープンソースの SLAM システムである VINS(Visual-Inertial Navigation System)-Fusion をベースとしたなりすまし検知手法を提案します。提案手法は、GNSS 測定値の変位の確認とマルチセンサー推定から始まります。チェック後、提案手法は VINS-Fusion のローカル フレームとポーズ グラフ最適化から得られるグローバル フレームの変換行列を利用します。一般に、最適化のたびに変換行列がゆっくりと変化していることを考慮すると、行列の突然の変化はスプーフィング攻撃の発生を示している可能性があります。VINS-Fusion のパフォーマンスをテストして、ビジョンベースの状態推定システムにスプーフィング検出を実装する必要性を検証し、VINS-Fusion をスプーフィングの検出に使用できるかどうかを調査します。さらに、公開データセットを対象とした実験結果は、許容可能な誤報確率と検出ミス確率を備えた特定のスプーフィング シナリオにおけるスプーフィング検出方法の有効性を示しています。

追加情報:

オドメトリ(Odometry)は、通常、車両やロボットなどが移動する際に使用されるセンシング技術の一種です。オドメトリは、通常、車輪の回転や移動などの情報を使用して、移動した距離や方向などを推定するための手法を指します。

視覚オドメトリ: カメラやセンサーフュージョンなどを使用して、周囲の環境をモニタリングし、物体の変化に基づいて移動を追跡します。これは主にロボットビジョンなどで使用されます。

車輪オドメトリ: 車輪の回転に基づいて車両がどれだけ移動したかを計測します。通常、エンコーダーと呼ばれるデバイスが車輪の回転を検知し、その情報から移動距離や方向を推定します。

これらのオドメトリ情報は、位置推定、ナビゲーション、自己位置推定などのアプリケーションで使用されます。ただし、オドメトリは通常、時間の経過とともに誤差が蓄積するため、他のセンシング技術やシステムと組み合わせて使用され、より正確な位置情報を得るのに役立ちます。

VINS-Fusion(Visual-Inertial Navigation System Fusion)は、慣性センサー(主に加速度計とジャイロスコープ)と視覚センサー(カメラ)を組み合わせて、高精度な航法情報を提供するシステムです。これは慣性航法システム(Inertial Navigation System, INS)と視覚センシングを統合したものであり、特にロボティクス、ドローン、自律運転車、および拡張現実(AR)などの領域で利用されています。

Detect GNSS Spoofing Signals Using a Machine Learning Method

Patrick Xu, Curtis Hay, Rakesh Kumar, Iqbal Surti, Chandra Tjhai

Peer Reviewed

Abstract: Most Level 2 autonomous driving systems including General Motors (GM)' Advanced Driver Assistance System (ADAS) employ multiple sensors to achieve lane-level localization. As the only source onboard that provides absolute 3D global poses, Global Navigation Satellite Systems (GNSS) is susceptible to various Radio Frequency (RF) interferences such as jamming, spoofing and meaconing, intentionally or unintentionally. Since these interferences pose a growing threat to the safety and reliability of the automated vehicles, detecting, characterizing, and mitigating them become increasingly important. This paper proposes a machine learning-based method to detect spoofing signals. Basically, it treats the detection as a binary classification and evaluates the potential of applying supervised machine learning in the process. Various classifiers are trained and evaluated, and the best performing model is further optimized to predict the existence of interference signals. Raw GNSS measurements such as Pseudorange, Carrier Phase, Doppler, Clock Bias and Drift, Carrier-to-Noise Density (CN0), as well as their respective measurement uncertainties, are combined to train and test the machine learning models. Data cleaning, feature engineering, variable correlation analysis, and principal component analysis (PCA) were performed before the training process. Finally, to evaluate the effectiveness of the proposed method, two additional rounds of drive tests with real meaconing signals re-transmitted by multiple GNSS repeaters were performed at a GM vehicle testing facility in Michigan, US. Validation results showed an average of 97.4% detection accuracy, as well as an overall F1 score of 0.937.

Published in: Proceedings of the 2022 International Technical Meeting of The Institute of Navigation
January 25 - 27, 2022
Hyatt Regency Long Beach
Long Beach, California

機械学習手法を使用した GNSS スプーフィング信号検出

パトリック・スー、カーティス・ヘイ、ラケシュ・クマール、イクバル・スルティ、チャンドラ・ジャイ

ゼネラルモーターズ(GM)の先進運転支援システム(ADAS)を含むほとんどのレベル 2 自動運転システムは、車線レベルの位置特定を実現するために複数のセンサーを採用しています。全地球測位衛星システム（GNSS）は、絶対的な 3D 全球姿勢を提供するオンボードの唯一の情報源であるため、意図的か非意図的かにかかわらず、ジャミング、スプーフィング、ミーコンなどのさまざまな無線周波数（RF）干渉の影響を受けやすくなります。これらの干渉は自動運転車の安全性と信頼性に対する脅威を増大させるため、干渉を検出し、特徴付け、軽減することがますます重要になっています。この論文では、なりすまし信号を検出するための機械学習ベースの方法を提案します。基本的に、検出をバイナリ分類として扱い、そのプロセスで教師あり機械学習を適用する可能性を評価します。さまざまな分類器がトレーニングおよび評価され、最もパフォーマンスの高いモデルがさらに最適化されて干渉信号の存在が予測されます。擬似距離、搬送波位相、ドップラー、クロック バイアスとドリフト、搬送波対雑音密度（CN0）などの生の GNSS 測定値と、それぞれの測定の不確かさが組み合わされて、機械学習モデルのトレーニングとテストが行われます。データ クリーニング、特徴エンジニアリング、変数相関分析、および主成分分析（PCA）がトレーニング プロセスの前に実行されました。最後に、提案された方法の有効性を評価するために、米国ミシガン州の GM 車両試験施設で、複数の GNSS リピーターによって再送信された実際のミーコン信号による走行試験がさらに 2 回実施されました。検証結果は、平均 97.4% の検出精度と、全体的な F1 スコア 0.937 を示しました。

航海学会 2022 年国際技術会議議事録 2022 年
1 月 25 ～ 27 日
ハイアット リージェンシー ロングビーチ
カリフォルニア州ロングビーチ

Complex Cross Ambiguity Function Post-Decomposition Spoofing Detection with Inverse RAIM

Sahil Ahmed, Samer Khanafseh, Boris Pervan

Abstract: In this paper, we present decomposition results of the Complex Cross Ambiguity Function (CCAF) of spoofed Global Navigation Satellite System (GNSS) signals into their constitutive components [1]. We also propose a new, post-decomposition detection algorithm based on a new “inverse” Receiver Autonomous Integrity Monitoring (RAIM) concept. The goal is to differentiate the spoofed and the authentic satellite signals to generate an authentic navigation solution. First, each satellite provides the two sets of signal parameters (code phases) post-decomposition. Using combinations of these sets, we calculate the pseudorange residuals and identify the two consistent (the authentic and spoofed) navigation solutions among all possible signal combinations over different times. The method is applicable to spoofing scenarios that can lead to Hazardous Misleading Information (HMI) and are difficult to detect by other means. The method can identify spoofing in the presence of multipath and when the spoofing signal power matches with offsets in code delay and Doppler frequency relatively close to the true signal. Spoofing can be identified at an early stage within the receiver without additional augmented sensors.

Published in: Proceedings of the 35th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2022)
September 19 - 23, 2022
Hyatt Regency Denver
Denver, Colorado

Pages: 3443 - 3462

Cite this article: Ahmed, Sahil, Khanafseh, Samer, Pervan, Boris, "Complex Cross Ambiguity Function Post-Decomposition Spoofing Detection with Inverse RAIM," *Proceedings of the 35th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2022)*, Denver, Colorado, September 2022, pp. 3443-3462.
https://doi.org/10.33012/2022.18446

複雑な相互曖昧性関数 Inverse RAIM による分解後のスプーフィング検出

サヒル・アーメッド、サメール・カナフセ、ボリス・ペルヴァン

この論文では、なりすましの全地球航法衛星システム（GNSS）信号の複雑相互曖昧性関数（CCAF）を構成要素に分解した結果を示します [1]。また、新しい「逆」受信者自律整合性監視（RAIM）の概念に基づいた、新しい分解後検出アルゴリズムも提案します。目標は、なりすましの衛星信号と本物の衛星信号を区別して、本物のナビゲーション ソリューションを生成することです。まず、各衛星は分解後の 2 セットの信号パラメータ（コード位相）を提供します。これらのセットの組み合わせを使用して、擬似距離残差を計算し、さまざまな時点で考えられるすべての信号の組み合わせの中から 2 つの一貫した（本物とスプーフィングの）ナビゲーション ソリューションを特定します。この方法は、危険な誤解を招く情報（HMI）につながる可能性があり、他の手段では検出することが困難なスプーフィング シナリオに適用できます。この方法は、マルチパスが存在する場合、およびスプーフィング信号パワーがコード遅延および真の信号に比較的近いドップラー周波数のオフセットと一致する場合に、スプーフィングを識別できます。スプーフィングは、追加のセンサーを追加しなくても、受信機内の初期段階で特定できます。

第 35 回航法研究所衛星部門国際技術会議（ION GNSS+ 2022）の議事録 2022 年
9 月 19 ～ 23 日
ハイアット リージェンシー デンバー
コロラド州デンバー

補足説明：
Receiver Autonomous Integrity Monitoring（RAIM）は、航法や GPS（Global Positioning System）などの領域で使用される技術の一つです。RAIM は、GPS 受信機が自己完結して信頼性を確認し、誤差や障害に対処するための仕組みを指します。
GPS 受信機は、衛星信号の遅延、多重反射、大気中の異常伝播などによって生じる誤差に影響を受けます。RAIM は、これらの誤差や GPS 信号の異常を検知し、信頼性が確保されているかどうかを確認するための手法を提供しようとする仕組みを言います。

”Hazardous Misleading Information”（HMI）は、危険で誤解を招く情報を指す用語です。この用語は、特に航空機の運航や航法において重要です。航空業界では、HMI が提供されると、パイロットや関係者が安全に影響を与える可能性があります。
HMI は、例えば航空地図や気象情報、航空機の位置データなどで発生する可能性があります。これは、航空機が正確な情報に基づいて運航されることが極めて重要であるため、安全性に対する懸念が生じる可能性があり、危険な誤誘導情報が提供された場合、航空機関係者は正確な情報を確認し、それに基づいて適切な判断を下す必要があります。航空業界では、HMI を最小限に抑え、正確で信頼性の高い情報を提供することが求められています。

Robust Innovation-Based Spoofing Detection Method Against UE Maneuver in an INS/GNSS Integrated Navigation System

Yuhang Yang, Chao Sun, HongBo Zhao, Liyuan Zhang, Lu Bai

Abstract: Global Navigation Satellite Systems (GNSS) signals are susceptible to spoofing attacks, because of their open structure and weak power. Inertial navigation system (INS) is not affected by electromagnetic interference, which provides the INS/GNSS integrated system anti-spoofing capability. Innovation represents the difference between the pseudorange calculated by standalone GNSS and the priori estimate of pseudorange generated by the Kalman Filter. It can be employed to detect spoofing attacks. Various innovation-based spoofing detectors have been developed. However, in actual applications, it is found that the maneuver of user equipment (UE), such as a sudden turn or sudden acceleration, can also trigger the threshold of an innovation-based spoofing test statistic, leading to a very large probability of false alarm (Pfa). In this work, we address the problem of high false alarm rate due to UE maneuver by developing a specific force-aid spoofing detection algorithm. It employs the fact that the specific force will not be affected by spoofing, but will be affected by UE maneuvering. A new metric is developed, which is defined as the ratio of the sum of squares of normalized innovations and the sum of squares of specific force in horizontal directions. We evaluated the performance by both simulations and a hardware-based experiment. A dynamic driving test was carried out in Hainan, China. Results show that the proposed method significantly suppresses the high-PFA due to UE maneuver and meanwhile provides a slightly better spoofing detection performance than the conventional innovation-based method.

Published in: Proceedings of the 35th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2022)
September 19 - 23, 2022
Hyatt Regency Denver
Denver, Colorado

INS/GNSS 統合航法システムにおける UE 操作に対するロバストイノベーションベースのなりすまし検知手法

ユーハン・ヤン、チャオ・スン、ホンボ・チャオ、リユアン・ジャン、ルー・バイ

全地球航法衛星システム（GNSS）信号は、オープン構造で出力が弱いため、なりすまし攻撃を受けやすいです。慣性航法システム（INS）は電磁干渉の影響を受けないため、INS/GNSS 統合システムのスプーフィング防止機能が提供されます。イノベーションは、スタンドアロン GNSS によって計算された擬似距離と、カルマン フィルターによって生成された擬似距離の事前推定値との差を表します。スプーフィング攻撃を検出するために使用できます。さまざまなイノベーションベースのスプーフィング検出器が開発されています。しかし、実際のアプリケーションでは、急な方向転換や急加速などのユーザー機器（UE）の操作によっても、イノベーション ベースのスプーフィング テスト統計のしきい値がトリガーされ、非常に高い確率で誤った攻撃が行われる可能性があることが判明しています。アラーム発生確率（Pfa）が高いということです。この研究では、特定のフォースエイド スプーフィング検出アルゴリズムを開発することで、UE の操作による高い誤警報率の問題に対処します。これは、特定の力がスプーフィングの影響を受けないが、UE の操作によって影響を受けるという事実を利用しています。新しい指標が開発され、正規化されたイノベーションの二乗和と水平方向の比力の二乗和の比として定義されます。シミュレーションとハードウェアベースの実験の両方によってパフォーマンスを評価しました。動的走行テストは中国の海南省で実施されました。結果は、提案された方法が UE 操作による高 PFA を大幅に抑制し、一方で従来の革新ベースの方法よりわずかに優れたスプーフィング検出パフォーマンスを提供することを示しています。

第 35 回航法研究所衛星部門国際技術会議（ION GNSS+ 2022）の議事録 2022 年
9 月 19 ～ 23 日
ハイアット リージェンシー デンバー
コロラド州デンバー

補足説明：
”Probability of False Alarm”（Pfa）は、統計学や信号処理などの分野で使われる概念で、ある判定や検出が誤って警告（アラーム）を発する確率を示します。これは、実際には何も問題がないのに、システムが問題があると判断する確率を表します。

Pfaは以下の式で表されます：

$$Pfa = \frac{\text{False Alarms}}{\text{Total Trials}}$$

Session A5a: GNSS Security: Interference, Jamming and Spoofing 2

Assessment of Potential System Interference Through Radio Frequency Compatibility Analysis on Existing GNSS Frequencies by Emerging LEO Constellations

Himanshu Sharma, Dominik Doetterboeck, Thomas Pany, Universität der Bundeswehr München(ISTA)

Location: Seaview Ballroom

Date/Time: Thursday, Jan. 25, 1:50 p.m.

Peer Reviewed

Current trends in the space industry are shifting from Medium Earth Orbit (MEO) to Low Earth Orbit (LEO) constellations due to the cost-efficient launching capabilities of COTS-based HW resources. Several LEO systems currently offer a wide range of services, ranging from Broadband connectivity (e.g., Iridium, OneWeb, and Starlink) to the Internet of Things (IoT) applications (e.g., Hiber, Myriota, etc.). With the LEO constellation becoming popular, the scientific community is also exploring ways to maximize the use of LEO constellations in satellite-based positioning. The classic GNSS Systems like GPS (US), GLONASS (Russia), GALILEO (Europe), NAVIC (India), and QZSS (Japan), currently in operation, completely rely on MEO and/or GEO orbits. All satellite-based navigation systems from MEO and GEO have an orbit of at least 19,100 km above sea level, maximizing the signal attenuation due to path loss during signal propagation in space. In the past few years, LEO-PNT has emerged as a potential option for position estimation by using signals transmitted by LEO Constellations. Researchers have classified the use of the LEO constellation for position estimation in three broader terms (Prol, et al., 2022).

1) SoO Method: Considering LEO signals as a signal of opportunity (SoO). In this method, no dedicated positioning signals are transmitted by the satellites. It is the task of the receiver to use measurements such as angle of arrival (AOA), received signal strength or Doppler shift for position purposes. The researcher from the University (Placeholder1) of Texas Austin has applied a blind signal identification technique to uncover the frequency- and time-domain structure of the Starlink Ku-band downlink signal.

2) Modified-Payload Method: In this method, the LEO constellation dedicated to non-positioning purposes can have an additional payload needed for GNSS-like signal transmission. The receivers on the ground with some additional modification should be able to retrieve those signals and perform positioning tasks.

3) New LEO-PNT Method: A whole new constellation like a classic GNSS constellation with optimized design parameters for positioning and navigation purposes, is launched in the LEO orbit for positioning.

Considering all the approaches above from the receiver's perspective is a very cumbersome task. In case of a completely new signal transmitted by the LEO satellite, the receiver on the ground needs to adapt the front-end or in the worst case have a completely new front-end to process an additional signal. In mass market receivers (e.g., Smartphones), which share more than 80 % of GNSS receivers on earth (GSA, 2020), it is a very challenging task to accommodate such alternation in the GNSS front-end. Additionally, from the receiver manufacturer's point of view and considering hardware limitations for GNSS receiver frond-end, it will need a large amount of resources to adapt these new changes and bring them to the mass production level.

The other option that could be considered is that the LEO constellation, equipped with GNSS payload is transmitting in the same frequency band as used by classic GNSS systems. This method has the advantage that it is manufacturer friendly and the existing GNSS technology can be put to work immediately. However, the LEO constellation transmitting in the same frequency band must fulfill the international standard for interference in the framework of ITU defined in ITU-R M.1831 "A coordination methodology for RNSS inter-system interference estimation". This method provides a set of the figure of merits (FoM) (e.g., C/No degradation caused by the proposed system on the existing RNSS system). These parameters must fall within the threshold agreed internationally or by the mutual agreement between the two countries. Any country that wishes to plan its RNSS system must comply with these recommendations and threshold matrices before filing for the frequency usage to the ITU board, Thus, it is an uttermost important task to calculate these parameters beforehand and evaluate the interference effect caused by the proposed system on other existing systems.

The idea of this paper is to simulate realistic and potential LEO constellations transmitting in the frequency bands L1 and L5 and compute the main figure of merit described in ITU recommendation M.1831 ((ITU), 2015), the C/No degradation. Various parameters have a strong impact on the result, such as the aggregate gain of the visible satellites, the satellite antenna pattern, the transmit power, the center frequency of the LEO signals, and the modulation of the signals. The Institute of Space Technology and Space Application (ISTA) has developed a frequency compatibility tool in accordance with ITU-R M.1831 over the course of several years. The tool is fully capable of providing a Spectral Separation Coefficient (SSC) matrix, Interference values, effective C/No, C/No degradation, and several other figures of merits. The tool can perform both Analytical and Simulation-based approaches as mentioned in the ITU Recommendation.

The paper will be structured as follows. First potential constellations will be described based on planned constellations and meaningful candidates for PNT from LEO satellites. Secondly, signal candidates will be described and compared against existing GNSS signals. Then the methodologies to calculate the C/No degradation will be described in detail. Finally, results are shown in terms of degradation and margin with respect to the given transmit powers of the LEO signals.

新興 LEO 星座による既存の GNSS 周波数の無線周波数互換性分析による潜在的なシステム干渉の評価

ヒマンシュ・シャルマ、ドミニク・ドーターボック、トーマス・パニー、ミュンヘン連邦軍大学（ISTA）

宇宙産業の現在の傾向は、COTS ベースの HW リソースのコスト効率の高い打ち上げ能力により、中地球軌道（MEO）星座から低地球軌道（LEO）星座に移行しています。現在、いくつかの LEO システムは、ブロードバンド接続（Iridium、OneWeb、Starlink など）からモノのインターネット（IoT）アプリケーション（Hiber、Myriota など）に至る幅広いサービスを提供しています。LEO 星座の人気が高まるにつれ、科学界も衛星ベースの測位で LEO 星座を最大限に活用する方法を模索しています。現在運用されている、GPS（米国）、GLONASS（ロシア）、GALILEO（欧州）、NAVIC（インド）、QZSS（日本）などの古典的な GNSS システムは、完全に MEO および/または GEO 軌道に依存しています。MEO および GEO のすべての衛星ベースのナビゲーション システムは、海抜 19,100 km 以上の軌道を持ち、宇宙での信号伝播中の経路損失による信号の減衰を最大化します。ここ数年、LEO-PNT は、LEO コンステレーションによって送信された信号を使用した位置推定の潜在的なオプションとして浮上しました。研究者らは、位置推定のための LEO 星座の使用を 3 つの広い用語に分類しました（Prol, et al., 2022）。

1）SoO 法: LEO シグナルを機会シグナル（SoO）として考慮します。この方法では、衛星から専用の測位信号は送信されません。到来角（AOA）、受信信号強度、またはドップラー シフトなどの測定値を位置の目的に使用するのは、受信機の役割です。テキサス オースティン大学（Placeholder1）の研究者は、ブラインド信号識別技術を適用して、Starlink Ku バンド ダウンリンク信号の周波数領域および時間領域の構造を明らかにしました。

2）修正ペイロード方式: この方式では、測位以外の目的専用の LEO コンステレーションは、GNSS のような信号送信に必要な追加のペイロードを持つことができます。地上の受信機は追加の変更を加えれば、それらの信号を取得して測位タスクを実行できるはずです。

3）新しい LEO-PNT 方式: 測位とナビゲーションの目的で最適化された設計パラメータを備えた、古典的な GNSS コンステレーションのようなまったく新しいコンステレーションが、測位のために LEO 軌道に打ち上げられます。

受信者の観点から上記のすべてのアプローチを検討することは、非常に面倒な作業です。LEO 衛星によって送信されるまったく新しい信号の場合、地上の受信機はフロントエンドを適応させるか、最悪の場合には追加の信号を処理するためにまったく新しいフロントエンドを備える必要があります。地球上の GNSS 受信機の 80 % 以上を共有する大衆市場の受信機（スマートフォンなど）（GSA、2020）では、GNSS フロントエンドでこのような変更に対応することは非常に困難な作業です。さらに、受信機メーカーの観点から、GNSS 受信機フロントエンドのハードウェア制限を考慮すると、これらの新しい変更を適応させて量産レベルに引き上げるには、大量のリソースが必要になります。

考慮できるもう 1 つのオプションは、GNSS ペイロードを備えた LEO コンステレーションが、従来の GNSS システムで使用されているのと同じ周波数帯域で送信することです。この方法には、メーカーにとって使いやすく、既存の GNSS テクノロジーをすぐに活用できるという利点があります。ただし、同じ周波数帯域で送信する LEO コンステレーションは、ITU-R M.1831「RNSS システム間干渉推定の調整方法」で定義されている ITU の枠組みにおける干渉に関する国際標準を満たさなければなりません。この方法は、一連の性能指数（FoM）を提供します（たとえば、既存の RNSS システム上で提案されたシステムによって引き起こされる C/No 劣化）。これらのパラメータは、国際的に合意された、または二国間の相互合意によって定められた閾値内に収まらなければなりません。RNSS システムを計画したい国は、ITU 理事会に周波数使用を申請する前に、これらの推奨事項としきい値マトリックスに従わなければなりません。したがって、これらのパラメーターを事前に計算し、提案された周波数によって引き起こされる干渉の影響を評価することは、最も重要な作業です。他の既存システム上のシステム。この論文の目的は、周波数帯域 L1 および L5 で送信する現実的および潜在的な LEO コンステレーションをシミュレートし、ITU 勧告 M.1831（（ITU）、2015）に記載されている主要な性能指数である C/No 劣化を計算することです。可視衛星の総ゲイン、衛星アンテナ パターン、送信電力、LEO 信号の中心周波数、信号の変調など、さまざまなパラメーターが結果に大きな影響を与えます。Institute of Space Technology and Space Application（ISTA）は、ITU-R M.1831 に準拠した周波数互換性ツールを数年かけて開発しました。このツールは、スペクトル分離係数（SSC）マトリックス、干渉値、実効 C/No、C/No 劣化、およびその他のいくつかの性能指数を提供する完全な機能を備えています。このツールは、ITU 勧告で述べられているように、分析ベースのアプローチとシミュレーションベースのアプローチの両方を実行できます。

論文は以下のような構成となります。最初の潜在的な星座は、計画された星座と LEO 衛星からの PNT の意味のある候補に基づいて説明されます。次に、信号候補を説明し、既存の GNSS 信号と比較します。次に、C/No 劣化を計算する方法について詳しく説明します。最後に、LEO 信号の所定の送信電力に対する劣化とマージンの観点から結果を示します。

GNSS Spoofing Detection and Identification Based on Clock Drift Monitoring Using Only One Signal

Shunshun Shang, Hong Li, Yimin Wei, Mingquan Lu

Peer Reviewed

Abstract: In this paper, we propose a GNSS spoofing detection and identification method based on clock drift monitoring using only one signal. At present, there are many anti-spoofing techniques based on time information monitoring, such as clock bias and drift monitoring. However, these techniques estimate the time information using observations of at least four signals. As a result, they can only detect spoofing but cannot identify it. Besides, in order to estimate the time information, they need to solve a group of nonlinear equations iteratively, which requires a heavy computational load. In view of this, we propose a new method to estimate the clock drift using only one signal. Therefore, the proposed method can not only detect the spoofing signal but also identify it, and it can work normally even when authentic signals cannot be received. Furthermore, the method estimates the drift by solving a linear equation without any iteration, which has a lighter computational load compared to the previous methods. Experiments show that the method can detect and identify the spoofing signal when the spoofer moves, manipulates the time information, or is driven by an ordinary clock, such as a crystal clock.

Published in: Proceedings of the 2020 International Technical Meeting of The Institute of Navigation
January 21 - 24, 2020
Hyatt Regency Mission Bay
San Diego, California

Pages: 331 - 340

Cite this article: Shang, Shunshun, Li, Hong, Wei, Yimin, Lu, Mingquan, "GNSS Spoofing Detection and Identification Based on Clock Drift Monitoring Using Only One Signal," *Proceedings of the 2020 International Technical Meeting of The Institute of Navigation*, San Diego, California, January 2020, pp. 331-340.
https://doi.org/10.33012/2020.17147

1 つの信号のみを使用したクロック ドリフト監視に基づく GNSS スプーフィングの検出と識別
シャン・シュンシュン、ホン・リー、ウェイ・イーミン、ルー・ミンクアン

本稿では、1 つの信号のみを使用したクロックドリフト監視に基づく GNSS スプーフィングの検出および識別方法を提案します。現在、クロックバイアスやドリフト監視など、時間情報監視に基づくスプーフィング対策技術が数多く存在します。ただし、これらの技術は、少なくとも 4 つの信号の観測を使用して時間情報を推定します。その結果、なりすましは検出できるだけで、特定することはできません。さらに、時間情報を推定するには、一連の非線形方程式を繰り返し解く必要があり、大きな計算負荷がかかります。これを考慮して、我々は 1 つの信号のみを使用してクロック ドリフトを推定する新しい方法を提案します。したがって，提案手法はなりすまし信号の検出だけでなく識別も可能であり，正規の信号を受信できない場合でも正常に動作することができる。さらに、この方法は反復を行わずに線形方程式を解くことによってドリフトを推定するため、以前の方法と比較して計算負荷が軽くなります。実験によると、この方法は、スプーファーが移動したり、時間情報を操作したり、水晶時計などの通常の時計で駆動されたりしたときに、スプーフィング信号を検出および識別できることが示されています。

航海学会の 2020 年国際技術会議議事録 2020 年
1 月 21 ～ 24 日
ハイアット リージェンシー ミッション ベイ
サンディエゴ、カリフォルニア州

Session A5a: GNSS Security: Interference, Jamming and Spoofing 2

Charactering Receiver Clocks for the Detection and Identification of Inauthentic GNSS Signals

Zhen Zhu, East Carolina University Sanjeev Gunawardena, Air Force Institute of Technology Eric Vinande, Air Force Research Laboratory Jason Pontious, Air Force Research Laboratory

Location: Seaview Ballroom

Date/Time: Thursday, Jan. 25, 2:12 p.m.

Peer Reviewed

Receiver clock solution and the drift rate can be used to detect and identify the presence of inauthentic signals. In general, an inauthentic GNSS signal will carry the characteristics of its own local oscillator. It may be observed as part of the receiver clock solution.

The detection of inauthentic signals via a combination of receiver motion and clock solution was first explored in [1]. More recently, it was demonstrated in [2] and [3] that receiver clock drift can be monitored the time differenced carrier phase (TDCP) from a single satellite. Receiver motion can be compensated by IMU [3].

Alternatively, receiver motion and clock drift can be solved from a multi-GNSS TDCP solution. Our previous work in [4] showed that when TDCP is screened with Random Sample Consensus (RANSAC) algorithm, the solution can reach cm-level accuracy even in a GNSS-challenged environment. RANSAC can estimate the unknown parameters of the underlying model even when a significant portion of measurements is from outliers. It was originally proposed to identify an inlier set from noisy measurements in computer vision. Compared to the traditional RAIM methods, RANSAC can find consistency among a large number of measurements in an efficient way. Therefore, it is feasible to apply TDCP-based detection algorithms to a moving receiver even without an IMU. The detection algorithm could be individually implemented on every satellite in the measurement domain, or simultaneously on all visible satellites in the residuals of the TDCP solution equation.

In general, Random Sample Consensus will choose a measurement group that are consistent with each other. In theory, multiple inauthentic measurements could also be consistent with each other, for example, when they are created in the same simulator. Our previous results reported in [5] discussed the feasibility of detecting a group of simulated channels and differentiate them from the authentic ones in the TDCP solution, including clock drift. This work used a software defined radio receiver with a well-known Oven-Controlled Crystal Oscillator (OCXO).

Although the detection algorithm is applicable to TDCP measurements made with both SDR and commercial receivers, the quality of receiver clock must be considered. In general, if the receiver clock is low-noise and relatively stable, it becomes easier to detect the anomalies introduced by inauthentic signals. If the receiver clock has a predictable range of drift rate, it could help identify other clocks that were used to generate inauthentic signals.

In this work, we will examine the performance of clock drift solution estimated with TDCP using a commercial GNSS receiver. The receiver will be driven by different oscillator types, such as TCXO or OCXO. A TDCP-RANSAC solution will be computed with multi-constellation measurements recorded by this receiver. Using a combination of live signals and simulated signals, we will quantitatively assess the detectability of inauthentic signals based on clock drift solution, for each of the oscillators. Furthermore, we will explore the feasibility of identifying the clock model of the unknown simulator based on the TDCP-RANSAC solution and its residuals.

[1] P. Y. Hwang and G. A. McGraw, "Receiver Autonomous Signal Authentication (RASA) based on clock stability analysis," 2014 IEEE/ION Position, Location and Navigation Symposium - PLANS 2014, Monterey, CA, USA, 2014, pp. 270-281, doi: 10.1109/PLANS.2014.6851386.

[2] Shang, Shunshun, Li, Hong, Wei, Yimin, Lu, Mingquan, "GNSS Spoofing Detection and Identification Based on Clock Drift Monitoring Using Only One Signal," Proceedings of the 2020 International Technical Meeting of The Institute of Navigation, San Diego, California, January 2020, pp. 331-340. https://doi.org/10.33012/2020.17147

[3] Wood, Joshua, “Detection of GNSS Faults Using Receiver Clock Drift Estimates” Thesis, Auburn University, 2021. https://etd.auburn.edu//handle/10415/7749

[4] Zhu, Z., Vinande, E., Pontious, J. et al. (2022). A robust multi-constellation time-differenced carrier phase solution. GPS Solut 26, 8.

[5] Z. Zhu, S. Gunawardena, E. Vinande and J. Pontious, "Identification of Authentic GNSS Signals in Time-Differenced Carrier Phase Measurements with a Multi-Constellation Software Defined Radio Receiver," 2023 IEEE/ION Position, Location and Navigation Symposium (PLANS), Monterey, CA, USA, 2023, pp. 1027-1032, doi: 10.1109/PLANS53410.2023.10139922.

不正な GNSS 信号の検出と識別のための受信機クロックの特性評価

Zhen Zhu、イーストカロライナ大学 Sanjeev Gunawardena、空軍工科大学 Eric Vinande、空軍研究所 Jason Pontious、空軍研究所

日時:木曜日 1 月 25 日、午後 2 時 12 分

受信機クロック ソリューションとドリフト レートを使用して、不正な信号の存在を検出および識別できます。一般に、本物でない GNSS 信号は、それ自身の局部発振器の特性を伝えます。これは、受信機クロック ソリューションの一部として観察される場合があります。

受信機の動作とクロック ソリューションの組み合わせによる不正な信号の検出は、[1] で最初に検討されました。最近では、[2] および [3] で、単一衛星から受信機クロック ドリフトを時間差搬送波位相（TDCP）で監視できることが実証されました。受信機の動きは IMU によって補正できます [3]。

あるいは、受信機の動きとクロック ドリフトは、マルチ GNSS TDCP ソリューションから解決できます。[4] の以前の研究では、TDCP がランダム サンプル コンセンサス（RANSAC）アルゴリズムでスクリーニングされる場合、ソリューションは GNSS が困難な環境でも cm レベルの精度に達できることが示されました。RANSAC は、測定値のかなりの部分が外れ値によるものである場合でも、基礎となるモデルの未知のパラメーターを推定できます。当初は、コンピュータ ビジョンにおけるノイズの多い測定値からインライア セットを識別することが提案されました。従来の RAIM 手法と比較して、RANSAC は効率的な方法で多数の測定値間の一貫性を見つけることができます。したがって、IMU がなくても、移動する受信機に TDCP ベースの検出アルゴリズムを適用することが可能です。検出アルゴリズムは、測定ドメイン内のすべての衛星に個別に実装することも、TDCP 解方程式の残差内のすべての可視衛星に同時に実装することもできます。

一般に、ランダム サンプル コンセンサスでは、相互に一貫性のある測定グループが選択されます。理論的には、たとえば同じシミュレータで作成された場合など、複数の不正な測定値が相互に一致する可能性もあります。[5] で報告された以前の結果では、クロック ドリフトを含む、シミュレートされたチャネルのグループを検出し、TDCP ソリューション内の本物のチャネルと区別する実現可能性について説明しました。この研究では、よく知られたオーブン制御水晶発振器（OCXO）を備えたソフトウェア無線受信機を使用しました。

検出アルゴリズムは SDR と商用受信機の両方で行われる TDCP 測定に適用できますが、受信機クロックの品質を考慮する必要があります。一般に、受信機のクロックが低ノイズで比較的安定している場合、不正な信号によってもたらされた異常を検出することが容易になります。受信機クロックのドリフト レートが予測可能な範囲にある場合、不正な信号の生成に使用された他のクロックを特定するのに役立つ可能性があります。

この作業では、市販の GNSS 受信機を使用して TDCP で推定されたクロック ドリフト ソリューションのパフォーマンスを検証します。受信機は、TCXO や OCXO などのさまざまなタイプの発振器によって駆動されます。TDCP-RANSAC ソリューションは、この受信機によって記録されたマルチコンスタレーション測定値を使用して計算されます。ライブ信号とシミュレートされた信号の組み合わせを使用して、各発振器について、クロック ドリフト ソリューションに基づいて不正な信号の検出可能性を定量的に評価します。さらに、TDCP-RANSAC ソリューションとその残差に基づいて、未知のシミュレータのクロック モデルを識別する実現可能性を調査します。

Identification of Authentic GNSS Signals in Time-Differenced Carrier Phase Measurements with a Software Defined Radio

Zhen Zhu, Sanjeev Gunawardena

Abstract: Authentic and inauthentic GNSS signals could be differentiated in the carrier phase domain with the RANdom SAmple Consensus (RANSAC) algorithm. In this work, the algorithm is applied to measurements obtained with PyChips, a multi-frequency and multi-constellation GNSS SDR. RANSAC can be used to separate authentic signals from simulated or inauthentic ones in measurements from PyChips.

Published in: Proceedings of the 35th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2022)
September 19 - 23, 2022
Hyatt Regency Denver
Denver, Colorado

Pages: 3570 - 3579

Cite this article: Zhu, Zhen, Gunawardena, Sanjeev, "Identification of Authentic GNSS Signals in Time-Differenced Carrier Phase Measurements with a Software Defined Radio," *Proceedings of the 35th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2022)*, Denver, Colorado, September 2022, pp. 3570-3579.
https://doi.org/10.33012/2022.18453

ソフトウェア無線による時間差キャリア位相測定における本物の GNSS 信号の識別

ジェン・ジュー、サンジーブ・グナワルデナ

RANdom SAmple Consensus（RANSAC）アルゴリズムを使用すると、本物の GNSS 信号と本物でない GNSS 信号を搬送波位相ドメインで区別できます。この研究では、このアルゴリズムは、複数周波数および複数コンステレーションの GNSS SDR である PyChips で取得された測定値に適用されます。RANSAC を使用すると、PyChips からの測定において、本物の信号をシミュレートされた信号または本物でない信号から分離することができます。

補足説明:

RANSAC の基本的な概念:

RANSAC は、データセットに外れ値（ノイズや異常値）が存在する場合にも頑健なモデルを推定することを目的とします。

ランダムに一部のデータポイントを選択して仮のモデルを構築します。

選択されたポイントでモデルを適合させ、他のデータポイントと比較します。

ユーザーが設定した閾値内に収まるデータポイントを「インライア」（モデルにフィットする）と見なし、その数をカウントします。

上記の手順を一定回数繰り返し、最も多くのインライアを持つモデルを選択します

アルゴリズムの特徴:

RANSAC は、外れ値の影響を受けにくいため、ノイズの多いデータにも対応できます。確率的な手法であるため、ランダムなサンプリングに基づいているため、初期のサンプリングによって良好な結果が得られる確率が高まります。

Pychips は、2018 年からゼロから開発された比較的新しいオブジェクト指向の衛星ナビ SDR です。

以前の 2 つの実装、つまり Wideband TRIGR で配布された MATLAB SDR から得られた経験

（セクション V を参照）および MATLAB 用 ChameleonChips GNSS SDR ツールボックス（Gunawardena、2014）。

SDR の重要な約束の 1 つは、その柔軟性、したがって教育および研究ツールとしての有用性です。 ナビの文脈では、

公的に入手可能なさまざまな SDR を使用して、衛星ナビ システム、信号処理、および受信機設計に関する基本コースを教えることができます。ただし、学生がその特定の SDR に関連するプログラミング言語スキルを持っているという暗黙の前提があります。

学生は、SDR の内部動作を詳細に理解し、さらに重要なことに、SDR に変更を加えることが期待されています。

大学院研究プロジェクトの一環として、高度な機能やリビジョンを追加するためのコード。 これはある程度妥当ではありますが、

プログラミング言語の熟練度に関する仮定は、必ずしも当てはまらない場合があります。 さらに、状況を考慮すると、はるかに効率的である可能性があります

大学院生がプログラミングに時間を費やすよりも、研究をより深く進めることが有益です。

言語の専門家。 PyChips は、この概念をサポートするためにゼロから開発されました。

第 35 回航法研究所衛星部門国際技術会議（ION GNSS+ 2022）の議事録 2022 年

9 月 19 ～ 23 日

ハイアット リージェンシー デンバー

コロラド州デンバー

Synchronized Spoofing Attack Detection Using Galileo OSNMA and an Antenna Array

Markel Arizabaleta-Diez, Toms Dorins, Michai-Adrian Schipor, Thomas Pany, Universität der Bundeswehr München

Location: Seaview Ballroom

Date/Time: Thursday, Jan. 25, 2:35 p.m.

Peer Reviewed

Galileo open-service Navigation Message Authentication (OSNMA) is the first GNSS authentication service provided worldwide. The objective is to provide digital signature and additional authentication information (cryptography keys, key length, signature length, etc.) so that the user can authenticate the extracted navigation message from the Galileo satellites in view. The current paper presents the capabilities of the Galileo OSNMA to detect synchronized spoofing attacks performed by a commercial spoofing device. In addition to the Galileo OSNMA, a 3-element antenna array is employed for the spoofing attack detection. The goal is to evaluate both methods, to demonstrate that both methods are capable of determining a synchronized spoofing attack, and to identify the advantages and disadvantages of each method.

The current Galileo OSNMA requires the satellites to be connected to the ground station so that it can receive from the ground station the authentication data. When receiving the OSNMA data, the satellite incorporates the information in the I/NAV message, in the 40-bit OSNMA field, before the complete I/NAV message is broadcasted in Galileo E1-band. This means that not all Galileo satellites will transmit simultaneously OSNMA data. To allow the verification of those satellites not broadcasting OSNMA data bits, Galileo provides a cross-authentication between satellites. This means that the authentication data (e.g. digital signatures of the navigation data) of specific satellites is transmitted by another satellite. This allows a receiver to use the cross-authentication feature to verify all tracked satellites. The verification process with the OSNMA will state if a spoofing attack is happening by suffering continuous failures in the verification process. This would mean that something odd happens with the received signals, i.e., the receiver is being spoofed. The observed parameters related to OSNMA are the data availability for the

On the other hand, the multi-element antenna can also be used for spoofing detection. Within the paper, a six-element antenna will be employed. Among all the antenna-elements, only three are used for the reception of the signal. The received signals will then be processed by the Multi-Sensor Navigation Analysis Tool (MuSNAT), and the output of the phase-lock loops (PLLs) are employed to compute double differencing (DD). The DD method shows the phase offsets between the signals recorded different antennas, and therefore, when a spoofing happens, these phase offsets are expected to be inexistent, i.e., equal to zero. The DD is achieved by using master-slave tracking in MuSNAT, therefore the requirement of using 3 antenna-elements. In addition, each DD measurement requires two satellites, as one is required for reference purposes.

To perform the synchronized spoofing attack, a commercial jammer and spoofer device is employed. The device allows to perform various types of jamming and spoofing attacks, or even to combine them, by first jamming a receiver so that it can then be more easily spoofed. For the purpose of this paper, only the spoofing feature has been employed. The synchronized spoofing feature will then first need to extract the complete navigation message from the received signals-in-space (12 and 12.5 minutes for the Galileo and GPS signals, respectively) before it starts spoofing, i.e., it requires knowledge of what is been transmitted so that it provides coherent navigation data. As input parameters, prior information about the victim receiver (position and velocity) and the spoofing status (position and velocity that is desired) is required to achieve a successful synchronized attack. For simplicity, a static receiver has been used for the spoofing test. This paper also provides an analysis of the navigation data transmitted by the commercial spoofer during the synchronized spoofing attack.

The complete test set-up consists on a Trimble geodetic antenna located in the rooftop of the observatory of the UniBw M premises, which is connected to the commercial jammer and spoofer. The commercial spoofer output is connected to a directional antenna that transmits the spoofing signal. On the “victim” receiver side, the six-element antenna array is employed, from which only three-elements are connected to the recoding front-end. The recording front-end is a NI USRP 2955, which shares the same clock for all the three recording channels. The performed recording contains 5.5 minutes of real GNSS signals, then the spoofing is activated, which is transmitted with a higher power than the real signal for 8 minutes. Afterwards, the spoofing is deactivated, and therefore, the “victim” receiver will only receive the signals-in-space transmitted by the navigation satellites. All recorded channels are then processed by MuSNAT. The output of a single of these channels is employed to perform the OSNMA authentication, and all three channel outputs for verification for the multi-antenna DD technique.

The preliminary results show a successful detection of the spoofing with both OSNMA and DD. The first thing observed is that when the spoofer is activated, two new Galileo satellites are acquired and tracked. These new satellites were in view for the receiving antenna of the spoofer but were blocked by a building for the “victim” receiver. The second observation achieved is that while all GPS satellites managed to get spoofed, not all Galileo satellites were spoofed. The success or failure of spoofing the different satellites, could be observed by both OSNMA and DD. The DD showed the exact moment at which the spoofing takes over the tracking loops for those spoofed GPS and Galileo signals. When using OSNMA, as it requires retrieving the navigation message and the related authentication data and keys, the authentication failures are observed with a delay. A continuous failure in the authentication is then identified in this case as a spoofing attack. After showing analyzing both authentication methods, a trade off is performed based on the advantages and disadvantages of each technique.

Galileo OSNMA とアンテナ アレイを使用した同期スプーフィング攻撃の検出

マルケル・アリサバレタ＝ディエス、トムス・ドリンス、ミハイ＝アドリアン・シーポー、トーマス・パニー、ミュンヘン連邦軍大学

Galileo オープンサービス Navigation Message Authentication（OSNMA）は、世界中で提供される初の GNSS 認証サービスです。目的は、デジタル署名と追加の認証情報（暗号化キー、キーの長さ、署名の長さなど）を提供して、ユーザーが視界内の Galileo 衛星から抽出された航法メッセージを認証できるようにすることです。この文書では、商用スプーフィング デバイスによって実行される同期スプーフィング攻撃を検出する Galileo OSNMA の機能について説明します。Galileo OSNMA に加えて、スプーフィング攻撃の検出には 3 素子アンテナ アレイが採用されています。目標は、両方の方法を評価し、両方の方法が同期スプーフィング攻撃を判断できることを実証し、各方法の長所と短所を特定することです。

現在の Galileo OSNMA では、衛星が地上局から認証データを受信できるように地上局に接続する必要があります。OSNMA データを受信すると、完全な I/NAV メッセージが Galileo E1 バンドでブロードキャストされる前に、衛星はその情報を I/NAV メッセージの 40 ビット OSNMA フィールドに組み込みます。これは、すべての Galileo 衛星が同時に OSNMA データを送信するわけではないことを意味します。OSNMA データ ビットをブロードキャストしていない衛星の検証を可能にするために、Galileo は衛星間の相互認証を提供します。これは、特定の衛星の認証データ（たとえば、ナビゲーション データのデジタル署名）が別の衛星によって送信されることを意味します。これにより、受信機は相互認証機能を使用して、追跡されたすべての衛星を検証できるようになります。OSNMA による検証プロセスでは、検証プロセスで継続的に失敗することによってスプーフィング攻撃が発生しているかどうかが示されます。これは、受信信号に何か奇妙なことが起こっていること、つまり受信機がなりすましされていることを意味します。OSNMA に関連して観測されるパラメータは、OSNMA のデータ利用可能性です。一方、多素子アンテナはスプーフィング検出にも使用できます。この論文では、6 素子アンテナが使用されます。すべてのアンテナ素子のうち、信号の受信に使用されるのは 3 つだけです。受信信号はマルチセンサー ナビゲーション解析ツール（MuSNAT）によって処理され、フェーズ ロック ループ（PLL）の出力を使用して二重差分（DD）が計算されます。DD 法は、異なるアンテナで記録された信号間の位相オフセットを示すため、スプーフィングが発生した場合、これらの位相オフセットは存在しない、つまりゼロに等しいと予想されます。DD は、MuSNAT のマスター/スレーブ追跡を使用して実現されるため、3 つのアンテナ素子を使用する必要があります。さらに、各 DD 測定には 2つの衛星が必要です（参照目的で 1 つが必要です）。同期スプーフィング攻撃を実行するには、市販のジャマーおよびスプーファー デバイスが使用されます。このデバイスを使用すると、最初に受信機を妨害して、より簡単にスプーフィングできるようにすることで、さまざまなタイプのジャミング攻撃やスプーフィング攻撃を実行したり、それらを組み合わせたりすることができます。この文書では、スプーフィング機能のみが使用されています。同期スプーフィング機能は、スプーフィングを開始する前に、まず受信した宇宙信号から完全なナビゲーション メッセージを抽出する必要があります（ガリレオ信号と GPS 信号の場合はそれぞれ 12 分と 12.5 分）。つまり、何が行われているかについての知識が必要です。一貫したナビゲーション データを提供するために送信されます。同期攻撃を成功させるには、入力パラメータとして、被害者の受信機（位置と速度）とスプーフィングのステータス（目的の位置と速度）に関する事前情報が必要です。簡単にするために、スプーフィング テストには静的受信機が使用されています。このペーパーでは、同期スプーフィング攻撃中に商用スプーファーによって送信されたナビゲーション データの分析も提供します。完全なテスト セットアップは、UniBw M 施設の天文台の屋上にある Trimble 測地アンテナで構成され、市販の妨害装置とスプーファーに接続されています。商用スプーファ出力は、スプーフィング信号を送信する指向性アンテナに接続されています。「被スプーファ機側では、6 素子のアンテナ アレイが使用され、そのうちの 3 つの素子だけが記録フロントエンドに接続されます。録音フロントエンドは NI USRP 2955 で、3 つの録音チャンネルすべてで同じクロックを共有します。実行された録音には 5.5 分間の実際の GNSS 信号が含まれており、その後スプーフィングが有効になり、実際の信号よりも高い出力で 8 分間送信されます。その後、なりすましは無効化されるため、「被害者」受信機は航法衛星によって送信された宇宙信号のみを受信することになります。記録されたすべてのチャンネルは MuSNAT によって処理されます。これらのチャネルの 1つの出力は OSNMA 認証の実行に使用され、3 つのチャネル出力すべてはマルチアンテナ DD 技術の検証に使用されます。暫定的な結果は、OSNMA と DD の両方でスプーフィングの検出に成功したことを示しています。最初に観察されたのは、スプーファーが起動されると、2 つの新しいガリレオ衛星が捕捉され、追跡されるということです。これらの新しい衛星はスプーファーの受信アンテナの視界に入っていましたが、「被害者」受信機の建物によって遮られていました。2 番目に得られた観察は、すべての GPS 衛星がなんとかなりすましに成功したが、すべての Galileo 衛星がなりすましに成功したわけではないということです。さまざまな衛星のスプーフィングの成功または失敗は、OSNMA と DD の両方で観察できます。DD は、なりすましが GPS および Galileo 信号の追跡ループを引き継ぐ正確な瞬間を示しました。OSNMA を使用する場合、ナビゲーション メッセージと関連する認証データとキーを取得する必要があるため、認証の失敗は遅れて観察されます。この場合、認証が継続的に失敗すると、スプーフィング攻撃として識別されます。両方の認証方法の分析を示した後、各技術の長所と短所に基づいてトレードオフが実行されます。

Localizing the October 2022 Texas Jamming Incident Using ADS-B Data with an Improvement in Model Confidence

Zixi Liu, Juan Blanch, Sherman Lo, Todd Walter, Stanford University

Location: Seaview Ballroom

Date/Time: Thursday, Jan. 25, 2:58 p.m.

Peer Reviewed

GNSS serves several safety-of-life applications in aviation such as precise navigation for landing operations, collision avoidance, and Air Traffic Control (ATC). GNSS interference events happening near airports can severely affect safe operations in the airspace and can be hazardous for aircraft on approach or landing. Many interference events occur throughout the year, affecting US air traffic. A notable one is an interference event that happened at Dallas-Fort Worth International Airport (KDFW) in October/2022 which caused a widespread disruption. This incident resulted in multiple aircraft reporting GPS unreliable within 40NM of the airport, closure of a runway, and rerouting of air traffic. The source has still not been identified. Therefore, the main goal of this study is to solve the Texas mystery by providing our best estimate of when, where, what type, and how likely the interference source should be. The second goal of this study is to improve the model confidence of our localization algorithm. This helps ensure that even though the final estimated location might not be precisely the same as the underlying true jammer location, the corresponding error bound should have a size that is small enough to be used to narrow down the source location through a ground search.

In our previous study [1], we have performed detailed analysis on that incident using data from airborne receivers through Automatic Dependent Surveillance – Broadcast (ADS-B). Results from that study provide a better understanding of that event in terms of timeline and impact regions. We've identified some abnormal behaviors of the interference source, such as the jamming signal only affected airborne receivers (no ground reports), the size and shape of the impact region was changing over time, and there was a 5-hour gap in between the interference event. In this study, we analyze the underlying reasons for those phenomena to better understand what type of transmitter the potential jamming source should be. Another common cause of difficulty in identifying the source is the insufficient coverage of ADS-B reports, due to aircraft following similar flight paths. Therefore, we apply models that can extrapolate information from historical data to estimate signal conditions that are outside of the seen flight paths. Some commonly used models for extrapolation include Linear/Polynomial Regression, Bayesian Inference, and Neural Networks. We will identify which model has better performance when applying to this study and show how to modify the model to fit the usage of ADS-B reports.

In addition to improving the accuracy of localization algorithm, another thing that is also important is to improve the model confidence. We want to reduce the size of the error bound on the final result such that, even under abnormal conditions (such as this Texas incident), the final estimated location might not be precisely the same as the underlying true jammer location, the corresponding error bound should have a size that is small enough to help narrow down the source location through a search on the ground. Our ultimate goal is to design an algorithm that is able to provide Air Traffic Control with better situational awareness and to have interference sources to be quickly located and shut off.

[1] Liu, Z., Blanch, J., Lo, S., & Walter, T. (2023, January). Investigation of GPS Interference Events with Refinement on the Localization Algorithm. In Proceedings of the 2023 International Technical Meeting of The Institute of Navigation (pp. 327-338).

モデルの信頼性が向上した ADS-B データを使用した 2022 年 10 月のテキサス妨害事件の位置特定

Zixi Liu、Juan Blanch、Sherman Lo、Todd Walter、スタンフォード大学

GNSS は、着陸操作のための正確なナビゲーション、衝突回避、航空交通管制（ATC）など、航空分野における人命の安全を守るいくつかのアプリケーションに役立ちます。空港付近で発生する GNSS 干渉イベントは、空域での安全な運航に重大な影響を与える可能性があり、進入中または着陸中の航空機にとって危険となる可能性があります。年間を通じて多くの干渉イベントが発生し、米国の航空交通に影響を与えます。注目に値するのは、2022 年 10 月にダラス・フォートワース国際空港（KDFW）で発生し、広範囲にわたる混乱を引き起こした干渉イベントです。この事故により、複数の航空機が空港から 40NM 以内では GPS の信頼性が低いと報告し、滑走路が閉鎖され、航空交通のルートが変更されました。情報源はまだ特定されていない。したがって、この研究の主な目的は、干渉源がいつ、どこで、どのような種類で、どの程度の可能性があるのかについて最良の推定値を提供することで、テキサスの謎を解決することです。この研究の 2 番目の目標は、位置特定アルゴリズムのモデルの信頼性を向上させることです。これにより、最終的に推定された位置が基礎となる真の妨害電波の位置と正確に同じではない場合でも、対応する誤差限界のサイズが地上探索を通じて発信元の位置を絞り込むために使用できるほど十分に小さいことが保証されます。

私たちの以前の研究 [1] では、自動従属監視 - ブロードキャスト（ADS-B）を通じて航空機受信機からのデータを使用して、その事件の詳細な分析を実行しました。その研究の結果により、タイムラインと影響地域の観点からその出来事をより深く理解できるようになります。妨害信号が航空機の受信機にのみ影響を及ぼした（地上からの報告はなし）こと、衝突領域のサイズと形状が時間の経過とともに変化していたこと、衝突の間に 5 時間のギャップがあったことなど、干渉源の異常な動作をいくつか特定しました。干渉イベント。この研究では、潜在的な妨害源がどのような種類の送信機であるべきかをよりよく理解するために、これらの現象の根本的な理由を分析します。発生源の特定が困難になるもう 1 つの一般的な原因は、航空機が同様の飛行経路をたどるため、ADS-B レポートの対象範囲が不十分であることです。したがって、過去のデータから情報を外挿できるモデルを適用して、観測されている飛行経路の外側の信号状態を推定します。外挿によく使用されるモデルには、線形/多項式回帰、ベイジアン推論、ニューラル ネットワークなどがあります。この研究に適用する際にどのモデルのパフォーマンスが優れているかを特定し、ADS-B レポートの使用に合わせてモデルを変更する方法を示します。

位置特定アルゴリズムの精度を向上させることに加えて、モデルの信頼性を向上させることも重要です。私たちは、異常な状況（このテキサス州の事件など）の下でも、最終的な推定位置が基礎となる真の妨害電波の位置（対応する誤差限界）と正確に同じにならない可能性があるように、最終結果の誤差限界のサイズを削減したいと考えています。地上での探索を通じて発生源の場所を絞り込むのに役立つ十分な小さいサイズにする必要があります。私たちの最終的な目標は、航空交通管制に状況認識を向上させ、干渉源を迅速に特定して遮断できるアルゴリズムを設計することです。

[1] Liu, Z.、Blanch, J.、Lo, S.、および Walter, T.（2023 年 1 月）。位置推定アルゴリズムを改良した GPS 干渉イベントの調査。航海学会の 2023 年国際技術会議の議事録（pp. 327-338）。

場所:シービュー ボールルーム

日時: 1 月 25 日木曜日、午後 2 時 58 分

Investigation of GPS Interference Events with Refinement on the Localization Algorithm

Zixi Liu, Juan Blanch, Sherman Lo, Todd Walter

Peer Reviewed

Abstract: GNSS serves safety-of-life applications in aviation such as precise navigation for approach and landing operations. Interference events happen near airport can severely affect the safe operations of the airspace. A recent interference event happened at Dallas-Fort Worth International Airport (KDFW) on October/2022 caused a widespread disruption. This incident resulted in multiple aircraft reporting GPS unreliable within 40NM, closure of a runway, and rerouting of air traffic. In this study, we performed a detailed investigation on this event, and run our localization algorithm to provide an initial estimation of the potential jamming source. There were no public reports from ground infrastructures during this event, which means collecting data from the ground is not sufficient. Therefore, in this study, we used data collected from Automatic Dependent Surveillance—Broadcast (ADS-B) system. It is a satellite-based surveillance system on the airplane which broadcasts aircraft position information. ADS-B is already widely in use and was made mandatory in Europe and the U.S.A. by 2020. This ubiquity and openness of ADS-B provides widely available source of GNSS information. In addition to investigating Dallas event, this research also built on our previous work on localizing interference sources (Liu et al., 2022) and provided a method to calculate an error bound on the final estimated jammer location. In our prior research, we built an algorithm that can identify the most likely location and transmitted power of potential jammer in real time. In this work, we designed an algorithm to provide real-time confidence information about the localization result. The error bound calculated from this confidence monitoring scheme is compared with result from the bootstrap method (Stine, 1989). The goal of this design is to help narrow down the ground searching area in order to physically shut down the jamming source. We implemented and demonstrated this capability using recorded ADS-B transmissions from known interference events.

Published in: Proceedings of the 2023 International Technical Meeting of The Institute of Navigation
January 24 - 26, 2023
Hyatt Regency Long Beach
Long Beach, California

位置推定アルゴリズムの改良による GPS 干渉イベントの調査

ジーシー・リウ、フアン・ブランチ、シャーマン・ロー、トッド・ウォルター

GNSS は、進入および着陸操作のための正確なナビゲーションなど、航空における人命の安全を確保するアプリケーションに役立ちます。空港付近で干渉イベントが発生すると、空域の安全な運用に重大な影響を与える可能性があります。2022 年 10 月にダラス・フォートワース国際空港（KDFW）で発生した最近の干渉イベントは、広範囲にわたる混乱を引き起こしました。この事故により、複数の航空機が 40NM 以内では GPS が信頼できないと報告し、滑走路が閉鎖され、航空交通のルートが変更されました。この研究では、このイベントについて詳細な調査を実行し、位置特定アルゴリズムを実行して、潜在的な妨害源の初期推定を提供しました。このイベント中、地上インフラからの公的報告はありませんでした。これは、地上からのデータ収集が十分ではないことを意味します。したがって、この研究では、自動依存監視 - ブロードキャスト（ADS-B）システムから収集されたデータを使用しました。これは、航空機の位置情報をブロードキャストする、航空機上の衛星ベースの監視システムです。ADS-B はすでに広く使用されており、2020 年までにヨーロッパと米国で義務化されました。ADS-B のこの遍在性とオープン性により、広く利用可能な GNSS 情報ソースが提供されます。ダラスの事象の調査に加えて、この研究は干渉源の位置を特定するという以前の研究にも基づいており（Liu et al., 2022）、最終的に推定される妨害波位置の誤差限界を計算する方法を提供しました。私たちの以前の研究では、潜在的なジャマーの最も可能性の高い位置と送信電力をリアルタイムで特定できるアルゴリズムを構築しました。この研究では、ローカリゼーション結果に関するリアルタイムの信頼性情報を提供するアルゴリズムを設計しました。この信頼性監視スキームから計算された誤差限界は、ブートストラップ法（Stine、1989）の結果と比較されます。この設計の目的は、妨害源を物理的に遮断するために地上探索エリアを絞り込むことを支援することです。私たちは、既知の干渉イベントから記録された ADS-B 送信を使用してこの機能を実装し、実証しました。

航海学会の 2023 年国際技術会議の議事録 2023 年
1 月 24 ～ 26 日
ハイアット リージェンシー ロングビーチ
カリフォルニア州ロングビーチ

Preliminary Analysis of GNSS Radio Frequency Interference Events Detected in Canada and Impacts on GNSS Based Applications

Anurag Raghuvanshi, Sunil Bisnath, Jason Bond

Peer Reviewed

Abstract: Global Navigation Satellite Systems (GNSSs) transmit signals from space to Earth, enabling the determination of position, navigation and timing (PNT) information. National defence uses, safety-of-life applications and critical infrastructure (CI) sectors are just some of the areas that rely on PNT information provided by GNSS to improve safety and security, enable greater functionality, and increase productivity. PNT information has also become a fundamental enabler for many day-to-day applications ranging from the provision of directions while driving to fitness statistics on smartwatches to precision farming. This paper presents the findings of an in-depth analysis conducted on GNSS interference data collected from a specific site in Canada. The primary focus of this study was to examine the frequency, type, and severity of interference events observed at the site. The analysis provides valuable insights into the use of detectors, the nature of interference encountered, their potential sources, and their impact on the site's operations. Furthermore, this paper presents GNSS receiver parameters that can be utilized for automatic interference detection, along with technical recommendations for future detection algorithms. The detectors at the site have proven effective in detecting various types of interference including narrow band, chirp and single tone. The interference has a significant effect on C/N_0, number of satellites tracked, receiver noise, etc. and a loss of lock of signals can be encountered.

Published in: Proceedings of the 36th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2023)
September 11 - 15, 2023
Hyatt Regency Denver
Denver, Colorado

カナダで検出された GNSS 無線周波数干渉イベントと GNSS ベースのアプリケーションへの影響の予備分析

アヌラグ・ラグヴァンシ、スニール・ビスナス、ジェイソン・ボンド

全地球航法衛星システム（GNSS）は宇宙から地球に信号を送信し、位置、ナビゲーション、およびタイミング（PNT）情報の決定を可能にします。国防用途、人命安全アプリケーション、重要インフラ（CI）分野は、安全性とセキュリティを向上させ、機能を向上させ、生産性を向上させるために GNSS によって提供される PNT 情報に依存する分野のほんの一部です。また、PNT 情報は、運転中の道案内からスマートウォッチのフィットネス統計、精密農業に至るまで、多くの日常アプリケーションを実現するための基本的な要素となっています。このペーパーでは、カナダの特定の場所から収集された GNSS 干渉データに対して実施された詳細な分析の結果を紹介します。この研究の主な焦点は、現場で観察された干渉イベントの頻度、種類、重大度を調査することでした。この分析により、検出器の使用、遭遇した干渉の性質、潜在的な発生源、サイト運営への影響についての貴重な洞察が得られます。さらに、このペーパーでは、自動干渉検出に利用できる GNSS 受信機パラメータと、将来の検出アルゴリズムに関する技術的推奨事項を示します。現場の検出器は、狭帯域、チャープ、シングルトーンを含むさまざまなタイプの干渉を検出するのに効果的であることが証明されています。干渉は C/N_0、追跡される衛星の数、受信機のノイズなどに重大な影響を及ぼし、信号のロックの喪失が発生する可能性があります。

第 36 回航法研究所衛星部門国際技術会議（ION GNSS+ 2023）の議事録 2023 年
9 月 11 ～ 15 日
ハイアット リージェンシー デンバー
コロラド州デンバー

U.S. Department of Transportation (DOT) Global Positioning System (GPS) Interference Detection and Mitigation (IDM) Program

James S. Aviles, Karen L. Van Dyke

Abstract: Global Positioning System (GPS) Based Positioning, Navigation, and Timing (PNT) services support the United States transportation sector in safely transporting people and goods and enabling efficiencies resulting in benefits to national and economic security. GPS signals are broadcasted from a constellation of satellites orbiting in Medium Earth Orbit (MEO) and their signal strength at the user receiver is very low in signal power density magnitude and thus susceptible to unintentional and intentional signal disruption or manipulation from undesired sources. Two recent real-world events in the transportation sector highlight the impacts related to the susceptibility of these GPS signal disruptions and the constant need to improve the GPS Interference Detection and Mitigation (IDM) posture of the Department of Transportation with the goal to restore GPS based PNT services to the expected levels of availability and reliability. This IDM mission goal contributes to an overall resilient PNT services posture when GPS is quickly restored to the expected normal operating conditions. On January 21, 2022, the GPS signal-in-space around the city of Denver, CO was degraded by the presence of unwanted emissions south of the Denver International Airport1 . Numerous aircraft, train stations, emergency response communication towers and medical messaging services detected and experienced varying levels of GPS signal reception degradation for a period of approximately 33 hours until the unwanted emissions source was positively identified and shut down. On October 17, 2022, the GPS signal-in-space around the cities of Dallas and Fort Worth, TX was degraded by the presence of unwanted emissions southwest from the Dallas-Ft. Worth International Airport. Numerous aircraft in the terminal and air route airspace detected and experience GPS signal reception degradation for a period of approximately 44 hours. Ground infrastructure recordings of GPS signal degradation effects were absent during the active event affecting aircraft. The unwanted emissions source ceased without positively being identified.

Published in: Proceedings of the 36th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2023)
September 11 - 15, 2023
Hyatt Regency Denver
Denver, Colorado

米国運輸省（DOT）全地球測位システム（GPS）干渉検出および軽減（IDM）プログラム

ジェームズ・S・アヴィルズ、カレン・L・ヴァン・ダイク

全地球測位システム（GPS）ベースの測位、ナビゲーション、およびタイミング（PNT）サービスは、米国の運輸部門が人や物品を安全に輸送し、国家および経済の安全保障につながる効率化を実現するのをサポートします。GPS 信号は、中地球軌道（MEO）を周回する衛星群からブロードキャストされ、ユーザー受信機での信号強度は、信号電力密度の大きさが非常に低いため、意図的および意図的でない信号の中断や、望ましくないソースからの信号操作の影響を受けやすくなります。運輸部門における最近の 2 つの現実の出来事は、これらの GPS 信号中断の影響の受けやすさと、GPS ベースの復旧を目標に運輸省の GPS 干渉検出および軽減（IDM）体制を改善する継続的な必要性に関連する影響を浮き彫りにしています。期待されるレベルの可用性と信頼性を実現する PNT サービス。この IDM ミッションの目標は、GPS が予想される通常の動作状態に迅速に回復する際に、全体的な回復力のある PNT サービス体制に貢献します。2022 年 1 月 21 日、コロラド州デンバー市周辺の空間内 GPS 信号は、デンバー国際空港以南の不要な放射の存在により低下しました 1。多くの航空機、鉄道駅、緊急対応通信塔、医療メッセージング サービスが、望ましくない放出源が確実に特定され停止されるまで、約 33 時間にわたってさまざまなレベルの GPS 信号受信低下を検出し、経験しました。2022 年 10 月 17 日、テキサス州ダラス市とフォートワース市周辺の GPS 宇宙信号は、ダラス-フォートワースから南西にある不要な放射の存在によって低下しました。ワース国際空港。ターミナルおよび空路の空域にある多数の航空機が GPS 信号受信の低下を検知し、約 44 時間にわたって受信状態が低下しました。航空機に影響を与えた活発な事象の間、GPS 信号劣化の影響に関する地上インフラの記録は存在しませんでした。不要な排出源は明確に特定されることなく停止しました。

第 36 回航法研究所衛星部門国際技術会議（ION GNSS+ 2023）の議事録 2023 年
9 月 11 ～ 15 日
ハイアット リージェンシー デンバー
コロラド州デンバー

Session A5a: GNSS Security: Interference, Jamming and Spoofing 2

Detecting and Localizing Space Based Interference on GNSS Signals using Machine Learning

Akshata Patil, R. Eric Phelts, Todd Walter, Stanford University; Steffen Thoelert, German Aerospace Center (DLR)

Location: Seaview Ballroom

Alternate Number 1

Peer Reviewed

GNSS relies on relatively low-power signals that are below the noise floor. As a result, they are very vulnerable to interference, which can significantly impact a receiver's ability to effectively track and utilize the signals for navigation. The effects range from degradation in the receiver's ability to generate accurate and reliable position solutions to rendering a receiver unable to acquire and track other GNSS signals at the same or nearby frequencies. And, while ground-based interference can cause problems for many in a given local area, space-based interferers are potentially problematic for users of GNSS around the world. And both can be challenging to detect and localize.

Ground-based interference may be relatively easy to identify with a single receiver, but it can originate from a wide range of possible local sources. Space-based interference can be more difficult to identify without widespread receiver networks. However, assuming such a network is in place (and records to the right kinds of data), identifying the source is more straightforward, but can still be a slow or tedious process.

In June of 2021, spectrum analysis data recorded by Trimble's network of 43 multiband receivers distributed across the US and Europe was used to detect an unusual power spike within the B3/E6 band at 1268.52 MHz. Further monitoring and analysis revealed a distinct interference pattern that eliminated the possibility of local jamming and instead pointed to a space-based origin. This was substantiated by the simultaneous impact on receivers across the entire network over a 24-hour span. This prior investigation involved manually observing and analyzing averaged FFT data and correlating it with LOS observables obtained from each receiver to identify the space-based source and its global trajectory.

This paper proposes to expand the prior work in several ways, First, it better characterizes the interference on B3I published previously and provides more insight into its effect on that signal. In addition, the potential effects of different types of interferers on various GNSS frequencies and modulations are modeled and simulated. Finally, this paper develops a method to identify space-based interference more quickly and efficiently. It is believed that this will help make existing or future global receiver networks more capable of detecting it and identifying the source.

機械学習を使用した GNSS 信号上の空間ベースの干渉の検出と位置特定

Akshata Putil、R. Eric Phelts、Todd Walter、スタンフォード大学。Steffen Thoerrt、ドイツ航空宇宙センター（DLR）

場所:シービュー ボールルーム

代替番号 1

GNSS は、ノイズ フロアを下回る比較的低電力の信号に依存します。その結果、信号は干渉に対して非常に脆弱になり、信号を効果的に追跡してナビゲーションに利用する受信機の能力に大きな影響を与える可能性があります。その影響は、正確で信頼性の高い位置ソリューションを生成する受信機の能力の低下から、受信機が同じ周波数または近くの周波数で他の GNSS 信号を取得および追跡できなくなるまで多岐にわたります。また、地上からの干渉は特定の地域の多くの人にとって問題を引き起こす可能性がありますが、宇宙からの干渉は世界中の GNSS ユーザーにとって潜在的に問題となる可能性があります。そして、どちらも検出して位置を特定するのが難しい場合があります。

地上ベースの干渉は、単一の受信機で比較的簡単に特定できる場合がありますが、考えられる広範囲のローカル発生源から発生する可能性があります。宇宙ベースの干渉は、広範な受信機ネットワークがなければ特定がより困難になる可能性があります。ただし、そのようなネットワークが整備されている（そして適切な種類のデータが記録されている）と仮定すると、ソースの特定はより簡単になりますが、それでも時間がかかる、または退屈なプロセスになる可能性があります。

2021 年 6 月、米国とヨーロッパに分散した 43 台のマルチバンド受信機の Trimble ネットワークによって記録されたスペクトル分析データを使用して、1268.52 MHz の B3/E6 帯域内の異常な電力スパイクを検出しました。さらなる監視と分析により、局所的な妨害の可能性が排除され、代わりに宇宙ベースの発生源を示す明確な干渉パターンが明らかになりました。これは、24 時間にわたるネットワーク全体の受信機への同時影響によって実証されました。この以前の調査では、平均化された FFT データを手動で観察および分析し、それを各受信機から取得した LOS 観測値と相関させて、宇宙ベースの発生源とその全球軌道を特定することが含まれていました。

このペーパーでは、以前の研究をいくつかの方法で拡張することを提案しています。まず、以前に公開された B3I 上の干渉をより詳細に特徴付け、その信号に対する干渉の影響についてのより多くの洞察を提供します。さらに、さまざまな種類の干渉源がさまざまな GNSS 周波数および変調に及ぼす潜在的な影響がモデル化され、シミュレーションされます。最後に、この論文は、空間ベースの干渉をより迅速かつ効率的に特定する方法を開発します。これにより、既存または将来のグローバル受信ネットワークの検出能力と発信元の特定能力が向上すると考えられています。

Session A4: GNSS Security: Interference, Jamming and Spoofing 1

Demonstration of Single-Satellite GNSS Spoofer Geolocation

Zachary Clements, University of Texas at Austin; Iain Goodridge, Spire Global; Patrick Ellis, Apple; Matthew J. Murrian, Spire Global; Todd E. Humphreys, University of Texas at Austin

Location: Seaview Ballroom

Date/Time: Thursday, Jan. 25, 8:35 a.m.

This paper details the demonstration of single-satellite single-pass geolocation of a terrestrial Global Navigation Satellite System (GNSS) spoofer from Low Earth Orbit (LEO). The traditional approach for GNSS security has been to develop onboard receiver spoofing detection and mitigation techniques. The future of GNSS security takes a more active approach: global accurate and persistent localization of the emitters threatening GNSS receivers. Receivers in LEO have the ultimate world-wide vantage point to detect and geolocate GNSS spoofing attacks. Accurate LEO-based single-receiver emitter geolocation is possible from Doppler measurements alone, provided the emitter is transmitting at a constant frequency and a carrier can be extracted by the receiver. The first condition is not true for GNSS spoofers, as they transmit signals whose carrier frequency contains an unknown time-varying frequency component that imitates the Doppler corresponding to each individual spoofed navigation satellite. This paper discusses a technique that exploits the spoofed clock drift to remove the unknown time-varying frequency component added by the spoofers so that a Doppler (range-rate) time history can be extracted for geolocation. This method is verified by a controlled experiment, in partnership with Spire Global, wherein a LEO-based receiver captures GNSS spoofing signals transmitted from a known ground station on a non-GNSS frequency band.

単一衛星 GNSS Spoofer 地理位置情報のデモンストレーション

テキサス大学オースティン校、Zachary Clements 氏。イアン・グッドリッジ、スパイア・グローバル、パトリック・エリス、アップル。マシュー・J・ムリアン、スパイア・グローバル、トッド E. ハンフリーズ、テキサス大学オースティン校

このペーパーでは、地球低軌道（LEO）からの地上の全地球航法衛星システム（GNSS）スプーファーの単一衛星シングルパス地理位置情報のデモンストレーションについて詳しく説明します。GNSS セキュリティに対する従来のアプローチは、オンボード受信機のなりすまし検出および軽減技術を開発することでした。GNSS セキュリティの将来には、より積極的なアプローチが採用されます。つまり、GNSS 受信機を脅かすエミッターのグローバルで正確かつ永続的な位置特定です。LEO の受信機は、GNSS スプーフィング攻撃を検出し、地理位置を特定するための究極の世界規模の有利な地点を獲得します。LEO ベースの単一受信機エミッターの正確な地理位置情報は、エミッターが一定の周波数で送信し、受信機で搬送波を抽出できる場合には、ドップラー測定のみから可能です。最初の条件は、GNSS スプーファーには当てはまりません。GNSS スプーファーは、個々のスプーフィングされた航法衛星に対応するドップラーを模倣する未知の時変周波数成分をキャリア周波数に含む信号を送信するからです。この論文では、スプーフィングされたクロック ドリフトを利用して、スプーファーによって追加された未知の時変周波数成分を除去し、地理位置情報のドップラー（距離レート）時刻歴を抽出できるようにする手法について説明します。この方法は、Spire Global と提携した制御実験によって検証されています。この実験では、LEO ベースの受信機が、非 GNSS 周波数帯域で既知の地上局から送信された GNSS スプーフィング信号を捕捉します。

場所:シービュー ボールルーム
日時: 1 月 25 日木曜日、午前 8 時 35 分

Session A4: GNSS Security: Interference, Jamming and Spoofing 1

A Cost-Efficient RFI Localization Approach to Detect GNSS Jamming and Spoofing

Michael Felux, Valentin Fischer, Sophie Jochems, Okuary Osechas, Manuel Waltert, Luciano Sarperi, Zurich University of Applied Sciences; Martin Strohmeier, Armasuisse

Location: Seaview Ballroom

Date/Time: Thursday, Jan. 25, 8:57 a.m.

Peer Reviewed

This paper introduces a novel method to identify the source of a Radio Frequency Interference (RFI) in an affordable and easily deployable way using UAVs. A payload consisting of two GNSS antennas and a directional antenna was attached to a UAV. A heading-capable GNSS receiver was fed with the signal of one GNSS antenna into the primary antenna port, and the combined signal of the directional antenna and the other GNSS antenna into the second antenna port as test statistic. In flight tests, the location of a jammer, i.e., the RFI source, was determined on the basis of the position and heading of the UAV using the difference of the average C/N0 values of the two antenna inputs. The heading of the UAV at which the proposed test statistic yields a maximum value, the direction towards the RFI source is established. The proposed method was tested in a field experiment consisting of two flights and involving a directional jammer, which was located approximately 1.5 km from the UAV. Results of the first test flight indicate that the heading corresponding to the spike in the test statistic correspond well to the true direction of the jammer. However, during the second test flight, when the directional antenna pointed at the source of RFI for short periods of time only, the test statistic showed more variation and a less distinct peak. Besides, the proposed setup was tested close to a 5G antenna to evaluate if the proximity of the frequency bands of 5G and GPS L1 signals affect the detection capability of the proposed measurement setup. The test statistic showed a discernible peak indicating significant interference with the test statistic. In this paper, the feasibility of the proposed method could be demonstrated.

GNSS 妨害とスプーフィングを検出するためのコスト効率の高い RFI 位置特定アプローチ

ミヒャエル・フェルクス、ヴァレンティン・フィッシャー、ソフィー・ヨッヘムス、オクアリー・オセシャス、マヌエル・ワルター、ルチアーノ・サルペリ　チューリッヒ応用科学大学。Martin Strohmeier、アルマススイス

このペーパーでは、UAV を使用して手頃な価格で簡単に導入可能な方法で無線周波数干渉（RFI）の原因を特定する新しい方法を紹介します。2 つの GNSS アンテナと 1 つの指向性アンテナで構成されるペイロードが UAV に取り付けられました。ヘディング対応 GNSS 受信機には、1 つの GNSS アンテナの信号がプライマリ アンテナ ポートに供給され、指向性アンテナともう 1 つの GNSS アンテナの結合信号がテスト統計として 2 番目のアンテナ ポートに供給されました。飛行試験では、妨害波、つまり RFI 発信源の位置は、2 つのアンテナ入力の平均 C/N0 値の差を使用して、UAV の位置と方位に基づいて決定されました。提案された試験統計が最大値をもたらす UAV の機首方位、つまり RFI 発信源への方向が確立されます。提案された方法は、UAV から約 1.5 km の位置にある指向性ジャマーを含む 2 つの飛行からなるフィールド実験でテストされました。最初のテスト飛行の結果は、テスト統計のスパイクに対応する機首方位が妨害電波の真の方向によく対応していることを示しています。ただし、2 回目のテスト飛行中に、指向性アンテナが短時間だけ RFI の発信源に向けられたとき、テスト統計はより多くの変動と、より明確なピークを示しませんでした。さらに、提案されたセットアップは、5G と GPS L1 信号の周波数帯域の近接性が提案された測定セットアップの検出能力に影響を与えるかどうかを評価するために、5G アンテナの近くでテストされました。検定統計量には、検定統計量との重大な干渉を示す識別可能なピークが示されました。この論文では、提案された方法の実現可能性を実証することができました。

ITM 2024
1/25

Authentication Security of Combinatorial Watermarking for GNSS Signal Authentication

Jason Anderson, Sherman Lo, Todd Walter

Abstract: Watermarking Signal Authentication is a technique where a GNSS provider cryptographically perturbs the spreading code to allow for limited cryptographic authentication of the signal. Several proposals and future studies exist or are underway to augment GNSS signals with this capability. This work reintroduces a generalized combinatorial watermarking function that affords a flexible pathway to cryptographically prove the authentication security of the signal with receiver observables. The security levels can be on-par with standard cryptographic security (e.g., 128-bit security) and require little or no additional use of the navigation data bandwidth. We show how our methods apply to signals of different designs and signal-to-noise ratios. From this work, one can design a Watermarking Signal Authentication scheme and the accompanying receiver to have high confidence in a signal's authenticity.

Published in: Proceedings of the 36th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2023)
September 11 - 15, 2023
Hyatt Regency Denver
Denver, Colorado

GNSS 信号認証のための組み合わせ透かしの認証セキュリティ

ジェイソン・アンダーソン、シャーマン・ロー、トッド・ウォルター

透かし信号認証は、GNSS プロバイダーが拡散コードを暗号的に混乱させて、信号の限定的な暗号認証を可能にする技術です。この機能を使用して GNSS 信号を強化するための提案や今後の研究がいくつか存在するか、進行中です。この研究では、受信機のオブザーバブルによる信号の認証セキュリティを暗号的に証明するための柔軟な経路を提供する、一般化された組み合わせ透かし機能を再導入します。セキュリティ レベルは、標準の暗号化セキュリティ（128 ビット セキュリティなど）と同等にすることができ、ナビゲーション データ帯域幅の追加使用をほとんどまたはまったく必要としません。私たちの方法がさまざまな設計と信号対雑音比の信号にどのように適用されるかを示します。この作業により、信号の信頼性に対して高い信頼性を持つ透かし信号認証スキームとそれに付随する受信機を設計できます。

第 36 回航法研究所衛星部門国際技術会議（ION GNSS+ 2023）の議事録 2023 年
9 月 11 ～ 15 日
ハイアット リージェンシー デンバー
コロラド州デンバー

Hybrid Autoencoder for Interference Detection in Raw GNSS Observations

Karin Mascher, Stefan Laller, Philipp Berglez

Peer Reviewed

Abstract: Malfunctions or failures in Global Navigation Satellite System (GNSS) services can result in significant personal, material, and financial damages. By an early identification of anomalous behavior in GNSS signals, timely countermeasures can be taken. However, most of interference monitoring or mitigation techniques are only applicable with the use of high-end receivers and require a certain level of knowledge to be used effectively. This paper presents a GNSS interference monitoring approach employing machine learning methodologies that can be utilized by users of any expertise level and with any type of GNSS receiver capable of outputting raw GNSS observations. By leveraging simple signal-to-noise ratio (SNR) observations, different hybrid autoencoder models, including denoising or variational autoencoder combined with recurrent neural network (RNN) models, are trained and tested on real jamming and spoofing events. The developed monitoring system is represented by a “traffic-lights” system, indicating the severity or level of concern associated with each detected anomaly. The results contain a comparison between different RNN-based autoencoder implementations and have been tested on input data from high-end to low-end GNSS receivers. The analysis of the test set showed that there is a 95% probability of catching anomalies. Additionally, when applied to other geodetic receiver types like u-blox or Javad GNSS receivers, similar results were achieved. However, smartphone data is subject to some limitations. Notably, missed anomalies are primarily attributed to the low transmitting power from the jamming and spoofing devices, which poses challenges for detection.

Published in: Proceedings of the 36th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2023)
September 11 - 15, 2023
Hyatt Regency Denver
Denver, Colorado

生の GNSS 観測における干渉検出のためのハイブリッド オートエンコーダ

カリン・マッシャー、ステファン・ララー、フィリップ・ベルグレズ

全地球測位衛星システム（GNSS）サービスの誤動作または障害は、重大な個人的損害、物的損害、および経済的損害を引き起こす可能性があります。GNSS 信号の異常な動作を早期に特定することで、タイムリーな対策を講じることができます。ただし、干渉モニタリングまたは軽減技術のほとんどはハイエンド受信機を使用する場合にのみ適用可能であり、効果的に使用するには一定レベルの知識が必要です。このペーパーでは、あらゆる専門知識レベルのユーザーが、生の GNSS 観測値を出力できるあらゆるタイプの GNSS 受信機を使用して利用できる、機械学習手法を採用した GNSS 干渉モニタリング アプローチを紹介します。シンプルな信号対雑音比（SNR）観測を活用することで、リカレント ニューラル ネットワーク（RNN）モデルと組み合わせたノイズ除去または変分オートエンコーダーなどのさまざまなハイブリッド オートエンコーダー モデルが、実際の妨害やスプーフィング イベントでトレーニングおよびテストされます。開発された監視システムは「信号機」システムに代表され、検出された各異常に関連する重大度または懸念レベルを示します。結果には、さまざまな RNN ベースのオートエンコーダー実装間の比較が含まれており、ハイエンドからローエンドの GNSS 受信機までの入力データに対してテストされています。テストセットの分析により、95% の確率で異常を検出できることがわかりました。さらに、u-blox や Javad GNSS 受信機などの他の測地受信機タイプに適用した場合も、同様の結果が得られました。ただし、スマートフォンのデータ通信には制限があります。特に、見逃した異常は主に妨害装置やなりすまし装置からの送信電力が低いことが原因であり、検出が困難になっています。

第 36 回航法研究所衛星部門国際技術会議（ION GNSS+ 2023）の議事録 2023 年
9 月 11 ～ 15 日
ハイアット リージェンシー デンバー
コロラド州デンバー

GNSS Fault Detection and Mitigation using Android IMU

Dong-Kyeong Lee, Trey Taylor, Dennis M. Akos, Jeonghyeon Yun, Yongrae Jo, Byungwoon Park

Peer Reviewed

Abstract: Applications of location information provided by Android devices have been expanding rapidly due its prevalence in the technology market. However, as the development focus of the Global Navigation Satellite Systems (GNSS) chipsets inside smartphones are not only accuracy, precision, and integrity, but also power consumption and size constraints, the Android GNSS hardware and software are more susceptible to signal attenuation and interference compared to high performance geodetic GNSS receivers. For example, the Android GNSS navigation engines are more vulnerable to the effects of signal multipath and experience more frequent carrier phase cycle slips in reduced GNSS signal quality environments such as urban canyons. Although standalone smartphone GNSS receivers have these limitations, some of the smartphones have access to additional sensors for accuracy and integrity support, such as accelerometers and gyroscopes. In this paper, the effectiveness of the accelerometers and gyroscopes inside Android devices, in supporting the standalone Android GNSS receivers will be investigated. The investigation will use the smartphone embedded sensors for device-independent performance that is not reliant on any other external sources of information. The additional sensors will be mixed with the GNSS measurements through a tightly-coupled extended Kalman filter, and potential faults will be flagged and mitigated using the innovation metrics. The GNSS measurements will be singled differenced to remove the effects of clock bias and drift on the filter. The orientation of the device will be determined using the accelerometer and gyroscope, and complemented using the GNSS measurements. Also, the thresholds for the innovation metrics will be computed using nominal open-sky data. The novelty of the paper will be looking at how the additional smartphone sensors can be used to improve the position solution from the smartphone, and also detect and mitigate potential faults in the GNSS measurements due to multipath or carrier phase cycle slips.

Published in: Proceedings of the 35th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2022)
September 19 - 23, 2022
Hyatt Regency Denver
Denver, Colorado

Android IMU を使用した GNSS 障害の検出と軽減

イ・ドンギョン、トレイ・テイラー、デニス・M・エイコス、ユン・ジョンヒョン、チョ・ヨングレ、パク・ビョンウン

Android デバイスが提供する位置情報のアプリケーションは、テクノロジー市場における普及により急速に拡大しています。ただし、スマートフォン内の全地球航法衛星システム（GNSS）チップセットの開発の焦点は、精度、精度、完全性だけでなく、消費電力とサイズの制約にもあるため、Android GNSS ハードウェアとソフトウェアは信号の減衰や干渉の影響を受けやすくなっています。高性能測地 GNSS 受信機と比較して。たとえば、Android GNSS ナビゲーション エンジンは信号マルチパスの影響に対してより脆弱であり、都市部の渓谷などの GNSS 信号品質が低下した環境では、キャリア位相サイクル スリップがより頻繁に発生します。スタンドアロンのスマートフォン GNSS 受信機にはこれらの制限がありますが、一部のスマートフォンでは、加速度計やジャイロスコープなど、精度と完全性をサポートする追加のセンサーにアクセスできます。このペーパーでは、スタンドアロンの Android GNSS 受信機をサポートする際の、Android デバイス内の加速度計とジャイロスコープの有効性を調査します。この調査では、他の外部情報源に依存しない、デバイスに依存しないパフォーマンスを実現するためにスマートフォンに組み込まれたセンサーが使用されます。追加のセンサーは、密結合された拡張カルマン フィルターを通じて GNSS 測定値と混合され、潜在的な障害にはフラグが立てられ、革新的なメトリクスを使用して軽減されます。GNSS 測定値は単一化されて差分化され、フィルター上のクロック バイアスとドリフトの影響が除去されます。デバイスの方向は加速度計とジャイロスコープを使用して決定され、GNSS 測定を使用して補完されます。また、イノベーション指標のしきい値は、名目上のオープンスカイ データを使用して計算されます。この論文の新規性は、追加のスマートフォン センサーを使用してスマートフォンからの位置ソリューションを改善する方法と、マルチパスまたはキャリア位相サイクル スリップによる GNSS 測定の潜在的な障害を検出して軽減する方法を検討することです。

第 35 回航法研究所衛星部門国際技術会議（ION GNSS+ 2022）の議事録 2022 年
9 月 19 ～ 23 日
ハイアット リージェンシー デンバー
コロラド州デンバー

GNSS spoofing detection through spatial processing

Fabian Rothmaier, Yu-Hsuan Chen, Sherman Lo, Todd Walter

Peer Reviewed

Abstract: In this paper, we present an algorithmic framework for signal-geometry-based approaches of GNSS spoofing detection. We formulate a simple vs. simple hypothesis test independent of nuisance parameters that results in significantly reduced missed detection probability compared to prior approaches. It is highly tractable such that it can be computed online by the receiver. We employ a hypothesis iteration framework that finds spoofed subsets of satellites efficiently and accounts for the presence of weak multipath, for a provable decision behavior in safety-of-life applications. We support the theoretical derivations by showing results on previously published simulated and on-air data sets. We validate the measurement model and show robustness to multipath with flight data from a Dual Polarization Antenna (DPA) mounted on a C12 aircraft. Finally, we show the algorithm's benefit on data recorded during a government-sponsored live spoofing event.

Video:

Published in: NAVIGATION: Journal of the Institute of Navigation, Volume 68, Number 2

Pages: 243 - 258

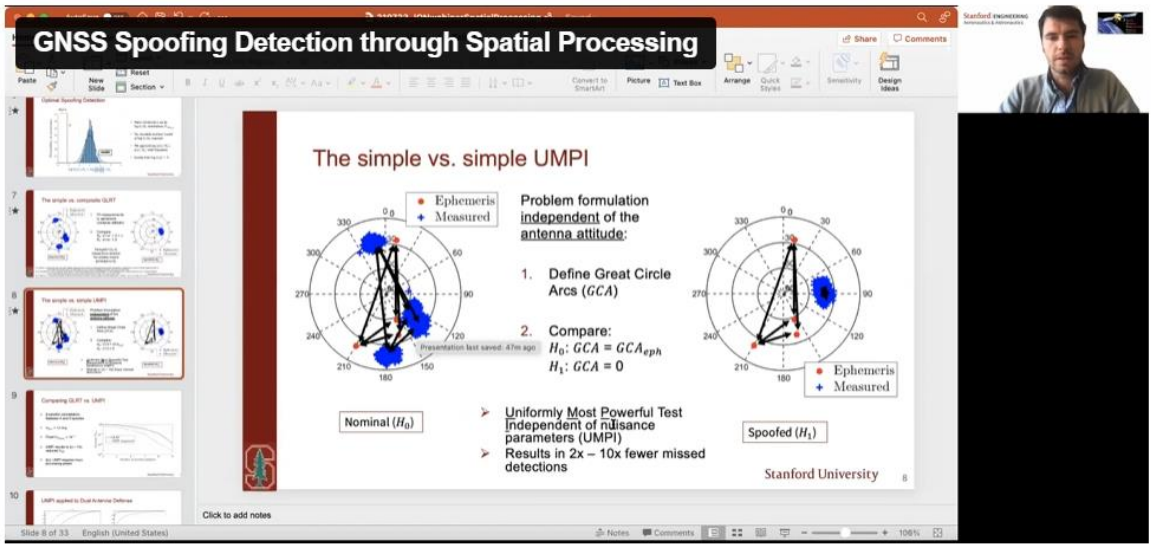
Cite this article: Citation Tools
https://doi.org/10.1002/navi.420

空間処理による GNSS スプーフィング検知

ファビアン・ロスマイヤー、ユーシュアン・チェン、シャーマン・ロー、トッド・ウォルター

この論文では、GNSS スプーフィング検出の信号ジオメトリ ベースのアプローチのためのアルゴリズム フレームワークを紹介します。迷惑パラメータに依存しない単純な仮説検定と単純な仮説検定を定式化することで、従来のアプローチと比較して検出ミスの確率が大幅に減少します。これは非常に扱いやすいため、受信者がオンラインで計算できます。私たちは、人命の安全アプリケーションにおける証明可能な意思決定動作のために、衛星のスプーフィングされたサブセットを効率的に見つけ、弱いマルチパスの存在を説明する仮説反復フレームワークを採用しています。以前に公開されたシミュレートされたデータセットとオンエアデータセットの結果を示すことで、理論的導出をサポートします。C12 航空機に搭載された二重偏波アンテナ（DPA）からの飛行データを使用して測定モデルを検証し、マルチパスに対する堅牢性を示します。最後に、政府主催のライブスプーフィング イベント中に記録されたデータに対するアルゴリズムの利点を示します。

ビデオ：



A Proposal for Securing Terrestrial Radio-Navigation Systems

Ronnie X.T. Kor, Peter A. Iannucci, Lakshay Narula, and Todd E. Humphreys

Peer Reviewed

Abstract: The security of terrestrial radio-navigation systems (TRNS) has not yet been addressed in the literature. This proposal builds on what is known about securing global navigation satellite systems (GNSS) to address this gap, re-evaluating proposals for GNSS security in light of the distinctive properties of TRNS. TRNS of the type envisioned in this paper are currently in their infancy, unburdened by considerations of backwards compatibility: security for TRNS is a clean slate. This paper argues that waveform- or signal-level security measures are irrelevant for TRNS, preventing neither spoofing nor unauthorized use of the service. Thus, only security measures which modify navigation message bits merit consideration. This paper proposes orthogonal mechanisms for navigation message encryption (NME) and authentication (NMA), constructed from standard cryptography primitives and specialized to TRNS: message encryption allows providers to offer tiered access to navigation parameters on a bit-by-bit basis, and message authentication disperses the bits of a message authentication code across all data packets, posing an additional challenge to spoofers. The implementation of this proposal will render TRNS more secure and resilient than traditional civil GNSS.

Published in: Proceedings of the 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2020)
September 21 - 25, 2020

Pages: 3313 - 3325

Cite this article: Kor, Ronnie X.T., Iannucci, Peter A., Narula, Lakshay, Humphreys, Todd E., "A Proposal for Securing Terrestrial Radio-Navigation Systems," *Proceedings of the 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2020)*, September 2020, pp. 3313-3325.
https://doi.org/10.33012/2020.17539

地上無線航法システムの安全確保に関する提案

ロニー XT コー、ピーター A. イアヌッチ、ラクシェイ ナルラ、トッド E. ハンフリーズ

地上無線航法システム（TRNS）のセキュリティについては、文献ではまだ取り上げられていません。この提案は、このギャップに対処する全地球航法衛星システム（GNSS）のセキュリティに関する既知の内容に基づいており、TRNS の独特の特性に照らして GNSS セキュリティの提案を再評価しています。この文書で想定されているタイプの TRNS は現在初期段階にあり、下位互換性を考慮する必要はありません。TRNS のセキュリティは白紙の状態です。この論文では、波形レベルまたは信号レベルのセキュリティ対策は TRNS には無関係であり、なりすましやサービスの不正使用を防ぐことはできないと主張しています。したがって、ナビゲーション メッセージ ビットを変更するセキュリティ対策のみが考慮に値します。この論文では、標準の暗号化プリミティブから構築され、TRNS に特化した、ナビゲーション メッセージ暗号化（NME）と認証（NMA）の直交メカニズムを提案します。メッセージ暗号化により、プロバイダーは、ビットごとのナビゲーション パラメーターとメッセージへの階層的なアクセスを提供できるようになります。認証では、メッセージ認証コードのビットがすべてのデータ パケットに分散されるため、スプーファーにとってさらなる課題となります。この提案の実装により、TRNS は従来の民間 GNSS よりも安全で復元力が高くなります。

第 33 回航法研究所衛星部門国際技術会議（ION GNSS+ 2020）議事録
2020 年 9 月 21 ～ 25 日

Barometer Based GNSS Spoofing Detection

Dong-Kyeong Lee, Filip Nedelkov, Dennis Akos, Byungwoon Park

Peer Reviewed

Abstract: In recent years, the number of smartphones with onboard Global Navigation Satellite System (GNSS) chipsets has been increasing. Although the navigation engines inside these phones use information from the GNSS chipsets as well as other sources of location such as network positioning, they are still vulnerable to GNSS spoofing. GNSS spoofing refers to the temperance of GNSS receivers using artificial GNSS signals to provide misleading positions, velocities, or time information. Failure to detect the presence of GNSS spoofing may result in the breach of integrity for systems using the navigation information from the GNSS receivers. There are several potential methods to detect GNSS spoofing for smartphones, including finding anomalies in the raw GNSS measurements and comparing the GNSS-based navigation solutions to inertial sensors. In this study, we explore the potential of utilizing the barometers inside smartphones to detect instances of GNSS spoofing. The advantages of using a barometer compared to other onboard GNSS-independent sensors include its potential to provide altitudes relative to the mean sea level, and its ability to provide high accuracy altitude rate data. In order to assess the capability of the barometers in GNSS spoofing detection, we assess the noise performances of both the barometers and the GNSS chipsets onboard smartphones under dynamic scenarios, and derive the thresholds for the discrepancy between the two sensors to establish acceptable levels of false detection. The novelty of this study lies in the improvement of the probability of false detection through local pressure corrections, carrier phase cycle slip mitigation, and filtering of both barometer and GNSS measurements using moving averaging and Kalman Filtering. Also, in the absence of local pressure corrections, the expected discrepancy bounds between the barometer, GNSS receiver, and truth due to spatial and temporal pressure variations are established as well. After the characterization of the thresholds, their performances are tested under real driving scenarios to simulate actual situations.

Published in: Proceedings of the 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2020)
September 21 - 25, 2020

気圧計ベースの GNSS スプーフィング検出

ドンギョン・リー、フィリップ・ネデルコフ、デニス・エイコス、ビョンウン・パーク

近年、全地球航法衛星システム（GNSS）チップセットを搭載したスマートフォンが増えています。これらの電話機内のナビゲーション エンジンは、GNSS チップセットからの情報だけでなく、ネットワーク測位などの他の位置情報源も使用しますが、依然として GNSS スプーフィングに対して脆弱です。GNSS スプーフィングとは、誤解を招く位置、速度、または時間情報を提供するために人工 GNSS 信号を使用する GNSS 受信機の抑制を指します。GNSS スプーフィングの存在を検出できないと、GNSS 受信機からのナビゲーション情報を使用するシステムの整合性が侵害される可能性があります。スマートフォンの GNSS スプーフィングを検出するには、生の GNSS 測定値の異常を検出する方法や、GNSS ベースのナビゲーション ソリューションを慣性センサーと比較する方法など、いくつかの方法が考えられます。この研究では、スマートフォン内の気圧計を利用して GNSS スプーフィングのインスタンスを検出する可能性を検討します。他の GNSS に依存しない車載センサーと比較して気圧計を使用する利点には、平均海面に対する高度を提供できる可能性と、高精度の高度率データを提供できる機能が含まれます。GNSS スプーフィング検出における気圧計の機能を評価するために、動的なシナリオの下で気圧計とスマートフォンに搭載された GNSS チップセットの両方のノイズ パフォーマンスを評価し、2 つのセンサー間の不一致のしきい値を導出し、偽の許容レベルを確立します。検出。この研究の新規性は、局所的な圧力補正、キャリア位相サイクルスリップの軽減、移動平均とカルマンフィルタリングを使用した気圧と GNSS 測定の両方のフィルタリングによる誤検出の確率の改善にあります。また、局所的な圧力補正がない場合、空間的および時間的な圧力変動による気圧計、GNSS 受信機、および真実の間の予想される不一致限界も同様に確立されます。しきい値の特性評価後、実際の運転シナリオの下でその性能がテストされ、実際の状況がシミュレートされます。

第 33 回航法研究所衛星部門国際技術会議（ION GNSS+ 2020）議事録
2020 年 9 月 21 ～ 25 日

A Tool for Furthering GNSS Security Research: The Oak Ridge Spoofing and Interference Test Battery (OAKBAT)

Austin Albright, Sarah Powers, Jason Bonior, Frank Combs

Abstract: A new global navigation satellite system (GNSS) dataset of digitized RF signals named the Oak Ridge Spoofing and Interference Test Battery (OAKBAT) has been created. OAKBAT contains digitized spoofing signals that serve as both a supporting “sibling,” and an advancement to the widely used Texas Spoofing Test Battery (TEXBAT) dataset [1]. OAKBAT at its core was developed to 1) allow for 100% reproducibility of the data, 2) provide more detailed metadata and contextual information about each dataset such as the precise moment the spoofing and/or interference signals begins, positions used, constellations visible, etc., and 3) to provide datasets generated using the same key parameters as the TEXBAT ds1 through ds6 datasets. Through these “sibling” datasets it will now be possible to determine if the behavior of algorithms and designs developed utilizing these datasets are affected by possible intrinsic behavior and properties of the equipment used in the generation and digitization of either of the two datasets. The end goal of OAKBAT is to be a new resource for the community of researchers and developers working in the field of GNSS. This additional source of data provides a GNSS “playground” on which to experiment, explore, and evaluate new ideas.

Published in: Proceedings of the 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2020)
September 21 - 25, 2020

GNSS セキュリティ研究を推進するツール: Oak Ridge スプーフィングおよび干渉テストバッテリー（OAKBAT）

オースティン・オルブライト、サラ・パワーズ、ジェイソン・ボニア、フランク・コムズ

Oak Ridge Spoofing and Interference Test Battery（OAKBAT）という名前の、デジタル化された RF 信号の新しい全地球航法衛星システム（GNSS）データセットが作成されました。OAKBAT には、サポートする「兄弟」として機能するとともに、広く使用されている Texas Spoofing Test Battery（TEXBAT）データセット［1］への進歩として機能するデジタル化されたスプーフィング信号が含まれています。OAKBAT の核心は、1）データの 100% の再現性を可能にする、2）スプーフィングや干渉信号が開始される正確な瞬間、使用される位置、表示される星座など、各データセットに関するより詳細なメタデータとコンテキスト情報を提供することを目的として開発されました。など、および 3）TEXBAT ds1 ～ ds6 データセットと同じキー パラメーターを使用して生成されたデータセットを提供します。これらの「兄弟」データセットを通じて、これらのデータセットを利用して開発されたアルゴリズムと設計の動作が、2 つのデータセットのいずれかの生成とデジタル化に使用される機器の潜在的な固有の動作と特性によって影響を受けるかどうかを判断できるようになります。OAKBAT の最終目標は、GNSS 分野で働く研究者や開発者のコミュニティのための新しいリソースとなることです。この追加のデータ ソースは、新しいアイデアを実験、探索、評価するための GNSS の「遊び場」を提供します。

第 33 回航法研究所衛星部門国際技術会議（ION GNSS+ 2020）議事録
2020 年 9 月 21 ～ 25 日

A Feasibility Study and Risk Assessment of Security Code Estimation and Replay (SCER) Attacks

Markel Arizabaleta, Elias Gkougkas and Thomas Pany

Abstract: The scope of the paper is to evaluate security code estimation and replay (SCER) attacks for GNSS signals. In the last years, many authentication methods have been presented to verify at the receiver that the incoming signal comes from the satellite. The authentication proposals can be divided in those that suggest the encryption of the navigation data, those that suggest the encryption of the spreading code sequence, and those that suggest a combination of both techniques. However, these techniques are still vulnerable against SCER attacks, which uses the estimation of the signal components in order to know the encrypted code and if required, modify it before retransmitting the signal. The primary goal of the investigation is to assess the feasibility of those attacks when applied on civil GNSS signals equipped with authentication features on spreading code level. For this purpose, different estimation techniques are taking into account and applied on different signal modulations received on different carrier to noise densities to illustrate the potential threat. For demonstration purposes, a parabolic dish antenna with a diameter of 2.4 m, which provides an antenna gain of 30 dBi, is used to illustrate the threat in real conditions. Furthermore, antenna arrays are also evaluated as alternative to using high-gain parabolic antennas. The scope of the current assessment is to define criteria and design drivers for future authentication components for open service users that are robust and resistant against attacks based on estimation and retransmission of partial or full encrypted spreading sequences.

Published in: Proceedings of the 32nd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2019)
September 16 - 20, 2019
Hyatt Regency Miami
Miami, Florida

セキュリティ コードの推定と再生（SCER）攻撃の実現可能性調査とリスク評価

マーケル・アリザバレタ、エリアス・グコウカス、トーマス・パニー

このペーパーの範囲は、GNSS 信号に対するセキュリティ コード推定およびリプレイ（SCER）攻撃を評価することです。ここ数年、受信信号が衛星からのものであることを受信機で検証するための多くの認証方法が提案されてきました。認証提案は、ナビゲーション データの暗号化を提案するもの、拡散コード シーケンスの暗号化を提案するもの、および両方の技術の組み合わせを提案するものに分類できます。ただし、これらの技術は、暗号化されたコードを知るために信号コンポーネントの推定を使用し、必要に応じて信号を再送信する前に変更する SCER 攻撃に対して依然として脆弱です。調査の主な目的は、拡散コード レベルの認証機能を備えた民間の GNSS 信号に適用された場合のこれらの攻撃の実行可能性を評価することです。この目的のために、潜在的な脅威を示すために、さまざまな推定手法が考慮され、さまざまな搬送波で受信されたさまざまな信号変調のノイズ密度に適用されています。デモンストレーションの目的で、30 dBi のアンテナ利得を提供する直径 2.4 m のパラボラ アンテナを使用して、実際の状況における脅威を示します。さらに、アンテナ アレイは、高利得パラボラ アンテナの使用に代わるものとしても評価されています。現在の評価の範囲は、部分的または完全に暗号化された拡散シーケンスの推定と再送信に基づく攻撃に対して堅牢で耐性のあるオープン サービス ユーザー向けの将来の認証コンポーネントの基準を定義し、ドライバーを設計することです。

The 32nd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2019)
2019 年 9 月 16 ～ 20 日
ハイアット リージェンシー
マイアミ フロリダ州マイアミ

The Use of Bearing Measurements for Detecting GNSS Spoofing

Peter F. Swaszek, Richard J. Hartnett, and Kelly C. Seals

Abstract: GNSS are well known to be accurate providers of position information across the globe. Because of high signal availabilities, robust receivers, and well-populated constellations, operators typically believe that the location information provided by their GNSS receiver is correct. More sophisticated users are concerned with the integrity of the derived location information; for example, employ RAIM algorithms to address possible satellite failure modes. The most common attacks on GNSS availability and integrity are known as jamming and spoofing. Jamming involves the transmission of signals that interfere with GNSS reception so that the receiver is unable to provide a position or time solution. Various methods to detect jamming, and possibly overcome it, have been considered in the literature. Spoofing is the transmission of counterfeit GNSS signals so as to mislead a GNSS receiver into reporting an inaccurate position or time. If undetected, spoofing might be much more dangerous than a jamming attack. A typical maritime concern is a spoofer convincing a tanker traveling up a channel to a harbor that it is off track of the channel. A variety of approaches have been proposed in the literature to recognize spoofing; many of these are based on the RF signal alone as, in some sense, they are the simplest to implement. Of interest here are methods which compare GNSS information to measurements available from other, non-GNSS sensors. Examined examples include IMUs, radars, and ranges/pseudoranges from non-GNSS signals. In all cases the data from these others sensors is compared to the position information from the GNSS receiver to assess its integrity. Triangulation of position from bearing measurements is a well-known localization technique, especially for the mariner. This paper considers the use of bearing information to detect GNSS spoofing in a 2-D environment. A typical marine application is a ship entering a harbor and using an alidade to sight landmarks; for mobile, autonomous vehicles the sensor might be a camera taking a bearing to a nearby vehicle or to a signpost. This paper presents a mathematical formulation of the problem and the sensor data, develops a statistical model of the measurements relative to the GNSS position output, constructs a generalized likelihood ratio test detection algorithm based on the Neyman-Pearson performance criterion (maximizing probability of detection while bounding the probability of false alarm), and examines performance of the test, both through analysis and experimentation. A comparison to using both range and bearing is included to show the utility and limitations of bearing data to spoof detection.

Published in: Proceedings of the 31st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2018)
September 24 - 28, 2018
Hyatt Regency Miami
Miami, Florida

GNSS スプーフィングを検出するための方位測定の使用

ピーター・F・スワゼック、リチャード・J・ハートネット、ケリー・C・シールズ

GNSS は、世界中で正確な位置情報を提供するものとしてよく知られています。高い信号可用性、堅牢な受信機、人口の多い星座のため、通信事業者は通常、GNSS 受信機によって提供される位置情報が正しいと信じています。より洗練されたユーザーは、派生した位置情報の整合性を重視します。たとえば、RAIM アルゴリズムを採用して、考えられる衛星障害モードに対処します。GNSS の可用性と整合性に対する最も一般的な攻撃は、ジャミングとスプーフィングとして知られています。ジャミングには、GNSS 受信を妨害する信号の送信が含まれ、受信機が位置または時間の解決策を提供できなくなります。ジャミングを検出し、おそらくそれを克服するためのさまざまな方法が文献で検討されています。スプーフィングとは、GNSS 受信機を欺いて不正確な位置または時刻を報告させるために、偽の GNSS 信号を送信することです。検出されない場合、スプーフィングはジャミング攻撃よりもはるかに危険である可能性があります。典型的な海事上の懸念は、海峡を遡って港に向かうタンカーに、海峡の軌道から外れていると信じ込ませるスプーファーです。スプーフィングを認識するためのさまざまなアプローチが文献で提案されています。これらの多くは、ある意味で実装が最も簡単であるため、RF 信号のみに基づいています。ここで興味深いのは、GNSS 情報を他の非 GNSS センサーから得られる測定値と比較する方法です。調査された例には、IMU、レーダー、非 GNSS 信号からの距離/擬似距離が含まれます。すべての場合において、これら他のセンサーからのデータは GNSS 受信機からの位置情報と比較され、その完全性が評価されます。方位測定値から位置を三角測量することは、特に船員にとってよく知られた位置特定手法です。このペーパーでは、2 次元環境で GNSS スプーフィングを検出するための方位情報の使用について検討します。典型的な海洋アプリケーションは、港に入港し、ランドマークを確認するためにアリダードを使用する船です。移動式の自動運転車の場合、センサーは近くの車両または標識の方位を取得するカメラである可能性があります。この論文では、問題とセンサー データの数学的定式化を示し、GNSS 位置出力に関連する測定値の統計モデルを開発し、ネイマン-ピアソン性能基準に基づいて一般化された尤度比テスト検出アルゴリズムを構築します（検出確率を最大化しながら、誤警報の確率を制限し、分析と実験の両方を通じてテストのパフォーマンスを検査します。スプーフィング検出に対する方位データの有用性と制限を示すために、距離と方位の両方を使用した場合の比較が含まれています。

第 31 回航法研究所衛星部門国際技術会議（ION GNSS+ 2018）の議事録 2018 年
9 月 24 ～ 28 日
ハイアット リージェンシー マイアミ
フロリダ州マイアミ

Resilient Timekeeping for Critical Infrastructure

John Fischer

Abstract: GNSS provides excellent time accuracy for synchronizing many commercial applications – datacenters, communication networks, power and process control operations, and more. However, when these applications are part of critical infrastructures, which many are, then the susceptibilities of GNSS to jamming and spoofing can undermine the operation. Resiliency is needed. This presentation will describe several ways that GNSS timing systems can be made more resilient for critical infrastructure. Specifically: 1. Interference Detection and Mitigation (IDM) techniques – analyzing the received GNSS signal can offer great insight into whether the signal is legitimate or not. The Dept. of Homeland Security has issued guidelines for protective measures for GPS receivers used in critical infrastructure, but additional methods are possible when all the GNSS constellations are considered. Also, advanced filtering techniques can eliminate some of the popular low-cost jamming signals in use today. 2. Anti-jam antennas – the best way to combat jamming and spoofing is not to allow the bad energy into the receiver in the first place. Directional, tracking and null steering antennas are available to block several types of jammers and spoofers but can become more costly as you add more protection. A cost-performance comparison will be shown along with real-world test results. 3. Augmentation with alternative signals such as Satellite Time and Location (STL) from Low Earth Orbit (LEO) constellations – though less accurate than GNSS, these much stronger signals provide a high level of interference and jamming protection. Moreover, the strong encryption protection is impervious to spoofing. These signals can be used in conjunction with GNSS to authenticate location (i.e., guarantee GNSS is not getting spoofed), as well as alone during periods of GNSS spoofing or denial. STL signals are available worldwide today. 4. Next Generation Receivers – multi-frequency, multi-constellation receivers are becoming more affordable for widespread commercial use. Some are beginning to offer machine learning techniques and advanced signal processing to further eliminate noise, multipath and interference. In addition, new services such as Open Service Navigation Message Authentication (OS-NMA) within Galileo will be operational in 2021. This will enhance protection against spoofing for any critical application. The state of the industry will be presented in this paper as it exists today and projected out into the next few years.

Published in: Proceedings of the 51st Annual Precise Time and Time Interval Systems and Applications Meeting
January 21 - 24, 2020
Hyatt Regency Mission Bay
San Diego, California

重要なインフラストラクチャのための回復力のある時間管理

ジョン・フィッシャー

GNSS は、データセンター、通信ネットワーク、電力およびプロセス制御操作など、多くの商用アプリケーションを同期するための優れた時間精度を提供します。ただし、これらのアプリケーションが重要なインフラストラクチャの一部である場合（多くはそうです）、GNSS は妨害やスプーフィングの影響を受けやすくなり、運用が損なわれる可能性があります。回復力が必要です。このプレゼンテーションでは、GNSS タイミング システムの重要なインフラストラクチャに対する回復力を高めるためのいくつかの方法について説明します。具体的には:

1. 干渉検出および軽減（IDM）技術 - 受信した GNSS 信号を分析すると、信号が正当なものかどうかについて優れた洞察が得られます。国土安全保障省は、重要インフラで使用される GPS 受信機の保護対策に関するガイドラインを発行しましたが、すべての GNSS コンステレーションを考慮すると、追加の方法も可能です。また、高度なフィルタリング技術により、現在使用されている一般的な低コストの妨害信号の一部を除去できます。

2. 妨害電波対策アンテナ - 妨害電波やなりすましに対抗する最善の方法は、そもそも受信機に悪いエネルギーを入れないようにすることです。指向性アンテナ、追跡アンテナ、およびヌル ステアリング アンテナは、数種類の妨害電波やスプーファーをブロックするために利用できますが、保護を追加するとコストが高くなる可能性があります。コストパフォーマンスの比較を実際のテスト結果とともに示します。3. 低地球軌道（LEO）星座からの衛星時刻と位置（STL）などの代替信号による補強 – GNSS よりも精度は劣りますが、これらのはるかに強力な信号は、高レベルの干渉と妨害からの保護を提供します。さらに、強力な暗号化保護により、なりすましの影響を受けません。これらの信号は、GNSS スプーフィングまたは拒否の期間中に単独で使用できるだけでなく、位置を認証する（つまり、GNSS がスプーフィングされていないことを保証する）ために GNSS と組み合わせて使用することもできます。STL 信号は現在世界中で利用可能です。4. 次世代受信機 – マルチ周波数、マルチコンステレーション受信機は、商業的に広く使用できるよう、より手頃な価格になりつつあります。ノイズ、マルチパス、干渉をさらに排除するために、機械学習技術と高度な信号処理を提供し始めている企業もあります。さらに、Galileo 内の Open Service Navigation Message Authentication（OS-NMA）などの新しいサービスが 2021 年に稼働する予定です。これにより、重要なアプリケーションのスプーフィングに対する保護が強化されます。このペーパーでは、業界の現在の現状と今後数年間の予測について説明します。

第 51 回年次精密時間および時間間隔システムおよびアプリケーション会議の議事録
2020 年 1 月 21 ～ 24 日
ハイアット リージェンシー ミッション ベイ
サンディエゴ、カリフォルニア州

An Anti-jamming and Anti-spoofing Digital Beamforming Platform for the GNSS-based ERTMS Train Control System

Alessandro Neri, Cosimo Stallo, Andrea Coluccia, Veronica Palma, Pietro Salvatori, Alessia Vennarini, Oscar Pozzobon, Giovanni Gamba, Samuele Fantinato, Mirko Barbuto, Alessio Monti, Filiberto Bilotti, Alessandro Toscano, Francesco Rispoli, Massimiliano Ciaffi

Abstract: The evolution plan of the European Railways Train Management System (ERTMS) includes the GNSS localization as one of the Game Changer technologies to improve the competitiveness of the ERTMS. GNSS will allow the implementation of cost-effective solutions to reduce the maintenance and operational cost without reducing the safety levels required by railway operations. The inherent low power of satellite navigation signals exposes GNSS-based solution to Radio Frequency threats, namely intentional or unintentional interference, that can lead to performance degradation or denial of service, and to spoofing/meaconing attacks, that can lead to receiver deception and hence to misleading PVT (Position, Velocity and Time) estimation. The aim of this paper is to present an architecture for detection and mitigation of radio-frequency hazards in a rail operational environment. The investigated solution is based on a Digital Beamforming Platform (DBP) coupled with advanced GNSS signal processing techniques for high rejection of GNSS interfering and counterfeit signals. This approach fully exploits the characteristics of the railway context, to support the evolution of the Location Determination System (LDS) based on GNSS in ERTMS Train Control System (TCS). This paper presents the DBP architectural design, focusing on the most meaningful and innovative solution foreseen for the prototype implementation. Each subsystem of the DBP is described in details, and a preliminary assessment of the performances is provided, by means of simulative and analytic tools.

Published in: Proceedings of the 30th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2017)
September 25 - 29, 2017
Oregon Convention Center
Portland, Oregon

GNSS ベースの ERTMS 列車制御システム用のアンチジャミングおよびアンチスプーフィング デジタル ビームフォーミング プラットフォーム

アレッサンドロ ネリ、コジモ スタッロ、アンドレア コルッチャ、ヴェロニカ パルマ、ピエトロ サルヴァトーリ、アレッシア ヴェナリーニ、オスカル ポッツォボン、ジョバンニ ガンバ、サミュエーレ ファンティナート、ミルコ バルブート、アレッシオ モンティ、フィリベルト ビロッティ、アレッサンドロ トスカーノ、フランチェスコ リスポリ、マッシミリアーノ チャッフィ

欧州鉄道列車管理システム（ERTMS）の進化計画には、ERTMS の競争力を向上させるゲーム チェンジャー テクノロジーの 1 つとして GNSS 位置特定が含まれています。GNSS を使用すると、鉄道運営に必要な安全レベルを低下させることなく、メンテナンスと運用のコストを削減するための費用対効果の高いソリューションの実装が可能になります。衛星航法信号の固有の低出力により、GNSS ベースのソリューションは、無線周波数の脅威、つまり、パフォーマンスの低下やサービス妨害につながる可能性のある意図的または非意図的な干渉、および受信機の欺瞞につながる可能性のある**スプーフィング/ミーコン攻撃**にさらされる可能性があります。誤解を招く PVT（位置、速度、時間）推定。このペーパーの目的は、鉄道の運用環境における無線周波数の危険を検出および軽減するためのアーキテクチャを提示することです。調査されたソリューションは、デジタル **ビームフォーミング** プラットフォーム（DBP）と高度な GNSS **信号処理**技術を組み合わせたもので、**GNSS 干渉信号や偽造信号を高度に除去します。**このアプローチは鉄道コンテキストの特性を最大限に活用し、ERTMS 列車制御システム（TCS）の GNSS に基づく位置決定システム（LDS）の進化をサポートします。このホワイト ペーパーでは、プロトタイプの実装で予見される最も有意義で革新的なソリューションに焦点を当てて、DBP アーキテクチャ設計について説明します。DBP の各サブシステムは詳細に説明されており、シミュレーションおよび分析ツールを使用してパフォーマンスの予備評価が提供されます。

第 30 回航法研究所衛星部門国際技術会議（ION GNSS+ 2017）の議事録 2017 年
9 月 25 ～ 29 日
オレゴン コンベンション センター
オレゴン州ポートランド

Real-time Pre-correlation Anti-jamming System for Civilian GNSS Receivers

Jorge Querol and Adriano Camps

Abstract: Global Navigation Satellite Systems (GNSS) have become a key technology that enables numerous location and navigation applications, thanks to the 24/7 worldwide availability of their signals, and the positioning accuracy that can be reached with them. However, GNSS have also some weaknesses, and the most relevant is that their signals reach the Earth's surface with very low power. This makes them quite vulnerable to the effect of Radio-Frequency Interference (RFI), and particularly to intentional jamming, which degrades, or even disrupts, the performance of the receivers. This problem is particularly threatening for those critical GNSS-enabled applications that trust on the integrity and continuity of GNSS signals, whose reliability may be committed. Such liability/security-critical civilian applications include autonomous aerial/terrestrial navigation, automatic rail signaling, geo-localized toll/insurance payments, or network synchronization among others. Moreover, RFI is also troublesome for derived GNSS applications such as GNSS-Reflectometry (GNSS-R) where GNSS signals are used as signals of opportunity in a multi-static radar configuration for Earth observation purposes. A number of mitigation solutions have been proposed to increase the continuity of GNSS signals in the presence of jamming signals. Regarding the structure of a GNSS system, the mitigation process can be performed at different stages: antenna, front-end, pre-correlation, post-correlation, or measurement. Common antenna solutions can provide spatiotemporal selectivity, which can reach interference rejection ration higher than 40 dB, but this is only achieved in static scenarios. On the contrary, pre-correlation techniques work at signal level, between antenna and GNSS correlators, providing interference selectivity in time, frequency, statistical, or other sub-space signal domains, which can mitigate jamming signals regardless the scenario dynamics. Moreover, pre-correlation techniques usually have a high computational burden in order to achieve high performance with interference rejection ratios higher than 30 dB. However, last generation Field Programmable Gate Arrays (FPGA) can overcome this drawback, and they even enable real-time pre-correlation anti-jamming solutions. The Front-End GNSS Interference eXcisor (FENIX) is a GNSS anti-jamming technology based on the patented combination of statistical interference detection, and a multiresolution time-frequency blanking algorithm for jamming mitigation in DSSS-based multi-constellation GNSS receivers [1]. The main goal of FENIX is to increase the C/N0 in the presence of interference signals, thus improving the continuity of GNSS services. Moreover, the mitigation algorithm has been designed to be DSSS-based multi-constellation, frequency independent (i.e. it works at L1 and L2, L5…), and it is capable of mitigating almost all kinds of jamming signals. A general description of the major building blocks of FENIX was first presented in [2]. This work aims at showing the implementation and first results of a real-time L1/L2 GPS/Galileo lite version of FENIX (FENIX-lite) tested using commercial jammers and GNSS receivers. The FENIX-lite demonstrator has been implemented using a two Software Defined Radio (SDR) model USRP B200mini, the first covers the GPS L1 C/A and Galileo E1 OS services, whereas the second does the same with the GPS L2C signal. The SDR front-ends are tuned to the L1 and L2 bands, and the FENIX interference detection and mitigation algorithm is running in real-time in both FPGA. The FENIX algorithm detects the interference signal using a statistical domain analysis based on normality tests, while the samples containing most part of interference power signal are excised in the time-frequency space computed using the Multiresolution Fourier Transform (MFT). The use of the MFT allows to mitigate almost of kinds of jamming signals since it maximized the projection of the interference signal in the transformed domain as demonstrated in [3]. In order to evaluate the improvement in the continuity of the GNSS signals, the degradation of the SNR with and without the FENIX-lite is compared using jammers at different bands and commercial GNSS receivers. [1] J. Querol, and A. Camps, "System and method for detecting and eliminating radio frequency interferences in real time," U.S. Patent Application 15 222 036, issued date July 28, 2016. [2] J. Querol, E. M. Julian, R. Onrubia, A. Alonso-Arroyo, D. Pascual and A. Camps, "Preliminary results of FENIX: Front-End GNSS Interference eXcisor," 2016 IEEE International Geoscience and Remote Sensing Symposium (IGARSS), Beijing, 2016, pp. 5627-5630. [3] J. Querol; R. Onrubia; A. Alonso-Arroyo; D. Pascual; H. Park; A. Camps, "Performance Assessment of Time-Frequency RFI Mitigation Techniques in Microwave Radiometry," in IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing, in press.

Published in: Proceedings of the 30th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2017)
September 25 - 29, 2017
Oregon Convention Center
Portland, Oregon

民生用 GNSS 受信機のためのリアルタイム事前相関アンチジャムのシステム

ホルヘ・ケロルとアドリアーノ・キャンプ

全地球航法衛星システム（GNSS）は、その信号が世界中で 24 時間年中無休で利用可能であり、測位精度が高いため、数多くの位置情報およびナビゲーション アプリケーションを可能にする主要なテクノロジーとなっています。ただし、GNSS にもいくつかの弱点があり、最も重要なのは、その信号が非常に低い出力で地表に到達することです。そのため、受信機は無線周波数干渉（RFI）の影響、特に受信機のパフォーマンスを低下させたり、さらには妨害したりする意図的な妨害に対して非常に脆弱になります。この問題は、信頼性が保証されている可能性がある GNSS 信号の完全性と連続性に依存する重要な GNSS 対応アプリケーションにとって特に脅威です。このような責任/セキュリティが重要な民間アプリケーションには、特に、航空/地上の自律ナビゲーション、自動鉄道信号、地理的にローカライズされた料金/保険の支払い、またはネットワーク同期が含まれます。さらに、RFI は、GNSS 信号が地球観測目的のマルチスタティック レーダー構成で機会信号として使用される GNSS 反射率測定（GNSS-R）などの派生 GNSS アプリケーションにとっても問題となります。妨害信号が存在する場合に GNSS 信号の連続性を高めるために、多くの緩和ソリューションが提案されています。GNSS システムの構造に関して、軽減プロセスは、アンテナ、フロントエンド、事前相関、事後相関、または測定などのさまざまな段階で実行できます。一般的なアンテナ ソリューションは時空間選択性を提供し、40 dB を超える干渉除去率に達することができますが、これは静的なシナリオでのみ達成されます。逆に、事前相関技術はアンテナと GNSS 相関器の間の信号レベルで機能し、時間、周波数、統計、またはその他のサブスペース信号ドメインで干渉の選択性を提供し、シナリオのダイナミクスに関係なく妨害信号を軽減できます。さらに、事前相関技術では、通常、30 dB を超える干渉除去率で高いパフォーマンスを達成するために、高い計算負荷がかかります。ただし、最終世代のフィールド プログラマブル ゲート アレイ（FPGA）ではこの欠点を克服でき、リアルタイムの事前相関妨害対策ソリューションも可能になります。フロントエンド GNSS 干渉 eXcisor（FENIX）は、統計的干渉検出と、DSSS ベースのマルチコンステレーション GNSS 受信機での妨害軽減のための多重解像度時間周波数ブランキング アルゴリズムの特許取得済みの組み合わせに基づく GNSS 妨害対策技術です［1］。FENIX の主な目標は、干渉信号の存在下で C/N0 を増加させ、GNSS サービスの継続性を向上させることです。さらに、軽減アルゴリズムは、DSSS ベースのマルチコンスタレーション、周波数に依存しないように設計されており（つまり、L1、L2、L5 などで動作します）、ほぼすべての種類の妨害信号を軽減できます。FENIX の主要な構成要素の一般的な説明は、[2] で最初に示されました。この研究の目的は、市販のジャマーと GNSS 受信機を使用してテストされた FENIX のリアルタイム L1/L2 GPS/Galileo ライト バージョン（FENIX-lite）の実装と最初の結果を示すことです。FENIX-lite デモンストレーターは、2 つのソフトウェア無線（SDR）モデル USRP B200mini を使用して実装されています。1 つ目は GPS L1 C/A および Galileo E1 OS サービスをカバーし、2 つ目は GPS L2C 信号で同じことを行います。SDR フロントエンドは L1 および L2 帯域に調整されており、FENIX 干渉検出および軽減アルゴリズムが両方の FPGA でリアルタイムで実行されます。FENIX アルゴリズムは、正規性テストに基づく統計領域分析を使用して干渉信号を検出し、干渉電力信号の大部分を含むサンプルは、多重解像度フーリエ変換（MFT）を使用して計算された時間周波数空間で削除されます。[3] で実証されているように、MFT を使用すると、変換された領域での干渉信号の投影が最大化されるため、ほとんどの種類の妨害信号を軽減できます。GNSS 信号の連続性の改善を評価するために、FENIX-lite を使用した場合と使用しない場合の SNR の低下を、さまざまな帯域のジャマーと市販の GNSS 受信機を使用して比較しました

第 30 回航法研究所衛星部門国際技術会議（ION GNSS+ 2017）の議事録 2017 年

9 月 25 ～ 29 日

オレゴン コンベンション センター

オレゴン州ポートランド

A Two-Step Beam-Forming Method Based on Carrier Phases for GNSS Adaptive Array Anti-Jamming

Hailong Xu, Xiaowei Cui, Jiannan Shen, Mingquan Lu

Abstract: Adaptive arrays have been widely used for interference mitigation in Global Navigation Satellite System (GNSS) receivers. Unlike adaptive nulling, adaptive beam-forming generates a dedicated beam in the antenna pattern towards each individual satellite and form nulls in the interference directions at the same time. Thus, the satellite signals are enhanced while interferences are mitigated, resulting in improved signal-to-interference-plus-noise ratio (SINR). In previous literature mainly two categories of beam-forming mechanisms are recommended, namely the array synthesis method and the so-called “blind” beam-forming method. The array synthesis method calculates the steering vector directly, but needs a cumbersome correction procedure dealing with the non-ideal factors of the antenna array and radio frequency (RF) channels. The blind beam-forming method generates the steering vector on-the-fly using carrier phases collected by auxiliary tracking channels, thus avoids the correction procedure, but has a limited performance against interferences. As an alternative, we proposed a different beam-forming method, which can be regarded as a combination of the two above. This method consists of two steps. In the calibration step, a carrier phase look up table (LUT) is obtained using the live-sky signals. In the beam-forming step, the steering vector is generated by looking up the LUT. This method doesn’t need a cumbersome non-ideal factor correction procedure, and has a good anti-interference performance, thus can be a third option for beam-forming. In order to implement and validate this method, a software-defined approach is used. Two real-time software receivers, one for the calibration step and one for the beam-forming step are designed and implemented. In order to meet the real-time requirement, a graphics processing unit (GPU) is used as an accelerator. A batched programming technique is used to fully take advantage of the parallelism offered by the GPU. Software design and programming details are introduced. Experiments are conducted in real environment and results are given. It concludes that this method has a good beam-forming performance in improving C/N0 and getting more precise positioning results.

Published in: Proceedings of the 2016 International Technical Meeting of The Institute of Navigation
January 25 - 28, 2016
Hyatt Regency Monterey
Monterey, California

GNSS アダプティブ アレイ アンチジャミングのためのキャリア位相に基づく 2 ステップのビームフォーミング手法

ヘイロン・シュー、シャオウェイ・クイ、ジャンナン・シェン、ミンクァン・ルー

アダプティブ アレイは、全地球航法衛星システム（GNSS）受信機の干渉軽減に広く使用されています。適応型ヌリングとは異なり、適応型ビーム フォーミングは、個々の衛星に向けてアンテナ パターンに専用のビームを生成し、同時に干渉方向にヌルを形成します。したがって、干渉が軽減されながら衛星信号が強化され、信号対干渉プラス雑音比（SINR）が向上します。以前の文献では、主に 2 つのカテゴリのビーム形成機構、すなわちアレイ合成法といわゆる「ブラインド」ビーム形成法が推奨されています。アレイ合成方法はステアリング ベクトルを直接計算しますが、アンテナ アレイと無線周波数（RF）チャネルの非理想的な要素を扱う面倒な補正手順が必要です。ブラインド ビーム フォーミング方法は、補助追跡チャネルによって収集された搬送波位相を使用してオンザフライでステアリング ベクトルを生成するため、補正手順が回避されますが、干渉に対するパフォーマンスは限られています。代替案として、上記 2 つの組み合わせとみなせる別のビームフォーミング方法を提案しました。この方法は 2 つのステップから構成されます。校正ステップでは、ライブスカイ信号を使用して搬送波位相ルックアップ テーブル（LUT）が取得されます。ビーム形成ステップでは、LUT を参照することによってステアリング ベクトルが生成されます。この方法は、面倒な非理想係数補正手順を必要とせず、優れた耐干渉性能を備えているため、ビームフォーミングの 3 番目のオプションとして使用できます。このメソッドを実装して検証するには、ソフトウェア定義のアプローチが使用されます。2 つのリアルタイム ソフトウェア受信機（1 つはキャリブレーション ステップ用、もう 1 つはビーム形成ステップ用）が設計され、実装されています。リアルタイム要件を満たすために、グラフィックス プロセッシング ユニット（GPU）がアクセラレータとして使用されます。GPU が提供する並列処理を最大限に活用するために、バッチ プログラミング手法が使用されます。ソフトウェア設計とプログラミングの詳細が紹介されます。実験は実際の環境で行われ、結果が得られます。この方法は、C/N0 を改善し、より正確な測位結果を得る上で優れたビームフォーミング性能を備えていると結論付けています。

航海学会 2016 年国際技術会議議事録 2016 年
1 月 25 ～ 28 日
ハイアット リージェンシー モントレー
カリフォルニア州モントレー

Evaluation of Mitigation Methods Against COTS PPDs

J. Rossouw van der Merwe, Alexander Rügamer, Fabio Garzia, Wolfgang Felber, Jan Wendel

Abstract: This paper analyzes the signals of different commercial-off-the-shelf (COTS) privacy protection devices (PPDs), and compares several mitigation algorithms applied to these jamming signals. A review of the mitigation algorithms is presented, including the theoretical requirements. This paper allows an end-to-end comparison of the algorithms in terms of the final performance versus the implementation requirements. The properties of the interference signal, specifically the dynamics of the signal, greatly affects the mitigation capability. For high interference-to-noise ratio (INR), the filter-bank pulse blanking (FBPB) had the best performance followed by the Dual-frequency-domain adaptive filtering (FDAF). It was also shown that the modulation of the satellite signal selection has a significant influence on the performance.

Published in: 2018 IEEE/ION Position, Location and Navigation Symposium (PLANS)
April 23 - 26, 2018
Hyatt Regency Hotel
Monterey, CA

Pages: 920 - 930

Cite this article: Merwe, J. Rossouw van der, Rügamer, Alexander, Garzia, Fabio, Felber, Wolfgang, Wendel, Jan, "Evaluation of Mitigation Methods Against COTS PPDs," *2018 IEEE/ION Position, Location and Navigation Symposium (PLANS)*, Monterey, CA, April 2018, pp. 920-930.

COTS PPD に対する緩和方法の評価

J. ロソウ・ファン・デル・メルヴェ、アレクサンダー・ルーゲーマー、ファビオ・ガルツィア、ヴォルフガング・フェルバー、ヤン・ウェンデル

このペーパーでは、さまざまな商用既製（COTS）プライバシー保護デバイス（PPD）の信号を分析し、これらの妨害信号に適用されるいくつかの軽減アルゴリズムを比較します。理論的要件を含め、緩和アルゴリズムのレビューが示されます。このペーパーでは、最終的なパフォーマンスと実装要件の観点からアルゴリズムをエンドツーエンドで比較できます。干渉信号の特性、特に信号のダイナミクスは、軽減能力に大きく影響します。高い干渉対雑音比（INR）の場合、フィルター バンク パルス ブランキング（FBPB）が最高のパフォーマンスを示し、次にデュアル周波数ドメイン適応フィルター（FDAF）が続きました。また、衛星信号選択の変調が性能に大きな影響を与えることも示されました。

2018 IEEE/ION Position, Location and Navigation Symposium（PLANS）
2018 年 4 月 23 ～ 26 日
ハイアット リージェンシー ホテル
モントレー、カリフォルニア州