時刻同期型 GNSS スプーフィングに対する IMU との複合航法を用いた検知指標検討

塩谷秀登（大阪府立大学大学院）
辻井利昭（大阪公立大学）

Time-synchronised GNSS spoofing detection index for combined GNSS/IMU navigation system

Hideto Shiotani (Osaka Prefecture University)
Toshiaki Tsujii (Osaka Metropolitan University)

Key Words: GNSS, spoofing, Inertial Measurement Unit, tightly coupled

Abstract

Global Navigation Satellite Systems (GNSS) are vulnerable to spoofing attacks. Therefore, in this study, GNSS / Inertial Measurement Unit (IMU) integrated navigation system was used to detect spoofing attacks. Specifically, we focused on signal strength and the variation in the standard deviation of the residual error.

1．はじめに

全球測位衛星システム(GNSS)は、簡単に測位が可能なシステムとして広く利用されている。しかし、民間の GNSS サービスは、衛星信号電力が熱雑音程度になる事から、他の電波の影響を容易に受ける。特に衛星信号になりすました偽の信号(スプーフィング信号)が送信された場合、受信機ユーザは攻撃者が意図する偽物の位置情報を本物と認識してしまうため、大きな障害を引き起こす恐れがある。

スプーフィングとは、偽の衛星信号を意図的に送信することで、目的の受信機を騙し、誤った位置情報や誤った時刻情報を生成させることを指す（図 1)。スプーフィングは、輸送、通信、軍事、金融など多くの分野のアプリケーションに対して潜在的な脅威となる可能性がある。

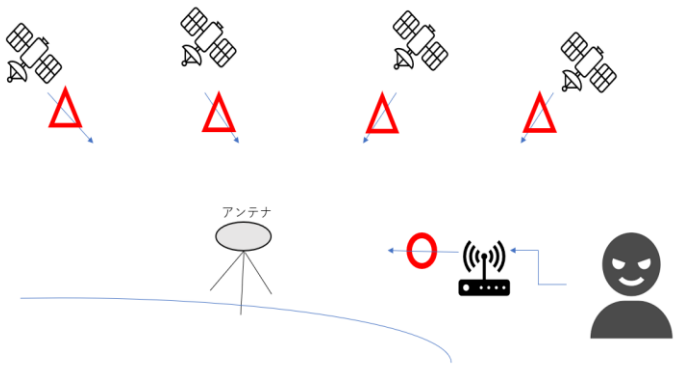

図 1　スプーフィングの概要

また、一般的な受信機では真の衛星信号とスプーフィング信号を見分けることは困難である。故に GNSS 信号に対するスプーフィング攻撃はユーザが気づかない可能性があるため、特に危険性が高く、対策を講じる必要がある。

実際に、スプーフィングによってヨットや航空機が GNSS を使用できなくなるなどの事例が度々報告されている。また今後登場する自動運転車もスプーフィングの影響を受ける可能性がある。自動運転車はマルチセンサを組み合わせているが、そのセンサのうち主要な PVT 源として扱われているものは GNSS 受信機である。スプーフィング攻撃を受けると、センサの累積誤差が増大し、事故に繋がる可能性がある。このようなスプーフィング攻撃への対応策として、本研究では、スプーフィング攻撃などの電波干渉を受けにくい独立した位置センサである IMU との複合航法を用いて、スプーフィング検知を目的とする[1]。

２．スプーフィング攻撃について

スプーフィング攻撃は、スプーフィングされた信号が本物の信号と時刻同期（コード位相に整合）しているかどうかに基づいて、非同期型スプーフィングと同期型スプーフィングに分類される。一般に時刻非同期型スプーフィングは、安価で誰でもその機器を入手可能であるのに対し、時刻同期型は特別な機器が必要である。その分、時刻同期型の方が検知されにくく、大きな被害が生じる可能性がある。つまり、スプーフィング攻撃を検知するならば、非同期型だけでなく、同期型も検知する必要がある。また、受信機は一般的に信号強度の強い信号をより追跡しやすいため、スプーフィング攻撃は目的の位置では本物の信号よりもわずかに大きい振幅を持つ必要がある。

２．１　時刻非同期型スプーフィング

非同期型スプーフィングは、時刻同期をせず、本物の信号との関係を考慮せずに任意のコンステレーションや事前に定義された軌道から測定値を生成し信号として送信するスプーフィング方法である。その中には、ミーコニング攻撃と分類され、別のところで受信した全ての GNSS 信号を増幅して再送信するものと、レコードアンドリプレイ攻撃と呼ばれる、数日前など過去に記録した信号を再送信するものなどが存在する。

今回の非同期型スプーフィングでは数日前に取得されたナビゲーションデータを用いて、GNSS シミュレータで偽の信号生成を行った。GNSS データは古く、本物の信号のコード位相とまったく一致していないため、スプーフィング信号とは相関ピークが何チップも離れている。このため、信号追尾の段階で簡単にスプーフィング信号にジャンプすることはない。しかし、スプーフィング信号のパワーを高く設定しているため（40dB 以上)、受信機のノイズフロアが上昇し、信号のロックが解除されるまで、本物の信号を妨害することが多くあった。受信機がいつどのように再捕捉するかは、受信機に依存するが、受信機に保存されているナビゲーションメッセージと照らし合わせ、スプーフィング信号と一致しないためその信号を全て測位に採用しない可能性も考えられる。今回スマートフォンを用いた実験では、スプーフィング信号によって妨害が続くケースと、数分後にスプーフィング信号に切り替わるケースがあった。実験では、5 分のスプーフィングファイルを送信していたが、より長いファイルであれば完全に切り替わる可能性も考えられる。

２．２　時刻同期型スプーフィング

時刻同期型スプーフィングはコード位相、ドップラーシフト、ナビゲーションビットなどの信号パラメータを可能な限り推定したスプーフィング方法である。同期型は目標とする受信機のリアルタイム位置を知っているため、信号遅延とドップラーシフトを一致させることが可能であり、リアルタイム位置を正確に把握できない場合は、非同期型のみ可能となる。相関ピークは非常に近く、スプーフィング信号のパワーが高ければ、本物の信号から相関ピークの切り替えが可能となる。実現するには、GNSS 情報をリアルタイムで取得し、受信機位置での各衛星信号の捕捉時刻を正確に把握するソフトウェア受信機及び、その航法データから時刻を同期した信号を生成するソフトウェア無線機が必要となる。非同期型スプーフィングと同期型スプーフィングの違いについて、以下の表 1 に示す[3]。P_s, P_a はそれぞれスプーフィング信号、真の信号の電力を表す。

表１　非同期型スプーフィングと同期型スプーフィングの比較

パラメータ	非同期型 スプーフィング	同期型 スプーフィング
信号電力	Ps＞Pa	Ps＜＜Pa → Ps＞Pa
コードシーケンス	本物の信号と厳密に同じ	
擬似距離	任意に決定	実信号と一致、その後 スプーファーに依存
搬送波位相	本物の信号と同じにするのは難しい	
時間	シミュレータ攻撃用に事 前に決定	本物の信号と照らし合 わせ同期
機器	・リピータ ・シミュレータ	・高度なリピータ ・スプーファー

3．時刻同期スプーフィング実験

JAXA 殿協力のもと、屋内で実衛星信号が受信可能なレドームで時刻同期スプーフィング実験を実施した。事前実験[4]で有効と見込まれた評価指標が実際のスプーフィング環境でも有効であるのか、検知可能であるのか以下の章で検証を行う。

3．1　使用機器

目標とする受信機は、スマートフォン（Galaxy S9）及び u-blox（EVK-M8）を用いた。IMU について、スマートフォンは内蔵されている IMU センサから加速度・角速度情報を取得し、u-blox との複合には GNAS モーションセンサ（東京航空計器）のデータを使用した。受信機の観測ファイルと IMU センサの加速度・角速度情報を統合する複合航法には、Tightly-coupled を用いた。スプーフィングによって、信号数が減少した場合であっても、複合を行えるように詳細なデータを扱う Tightly-coupled を採用した。偽の信号は CLAW-GPS シミュレータ（Jackson Labs Technologies）で生成した。スマートフォンに内蔵されている IMU センサ（LSM6DSL）及び、GNAS モーションセンサの精度を以下の表に示す。

	精度（3 軸加速度）	精度（3 軸角速度）
LSM6DSL	$\pm 0.89[m/s^2]$	$\pm 3.0[^\circ/s]$
GNAS モーションセンサ	$\pm 0.10[m/s^2]$	$\pm 0.50[^\circ/s]$

3．2　実験の概要

JAXA 調布航空宇宙センター飛行場分室の GNSS レドーム内で実験を行った。図 2 に簡易的なブロック線図を示す。実信号から受信した情報を基に時刻同期信号を GPS シミュレータに送信し、そのデータと事前にネットワークからダウンロードしておいたナビゲーションデータを統合し、時刻同期されたスプーフィング信号を生成する。

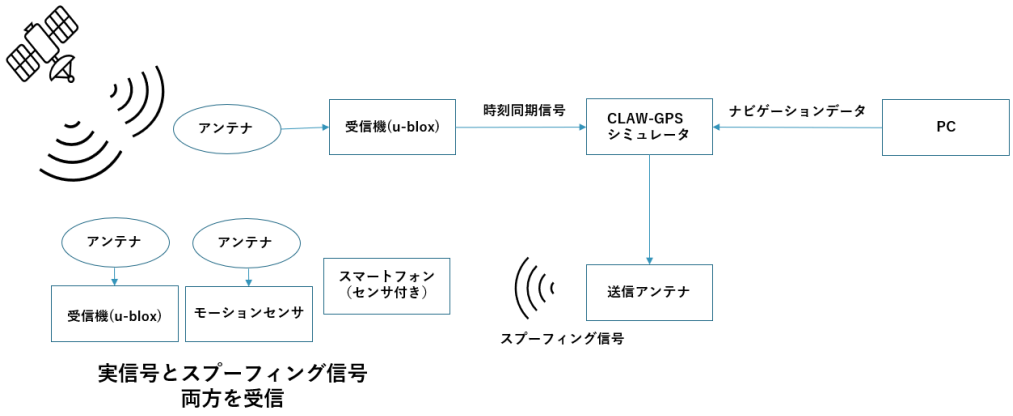

図 2　時刻同期スプーフィング実験のブロック線図

3．2　シミュレーション軌道

今回、受信機や IMU センサは全て静止状態で実験を実施した。実験のシナリオとして、1 分間実信号のみを受信した後、2 分間その場で静止する偽の GPS 信号を送信し、その後 3 分間偽の加速度運動及び、等速直線運動を行うようなスプーフィング信号を送信した。偽の信号のシミュレーション軌道を以下に示す。運動方向は南北方向のみである。1 本目の黒線が静止スプーフィング、2 本目の黒線が移動スプーフィング開始タイミングを表す。

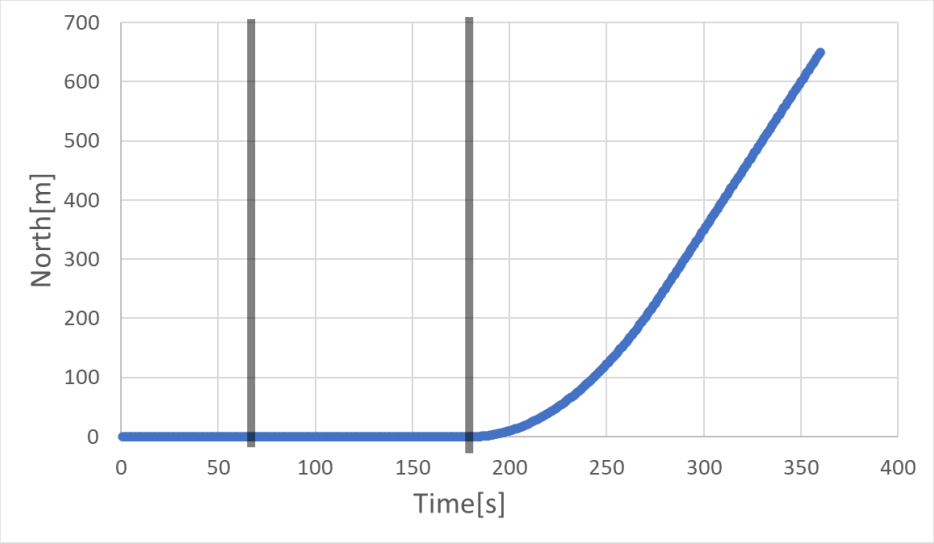

図 3　実装した偽のシミュレーション軌道（南北方向）
（60 秒後に静止スプーフィング送信、180 秒後に加速度運動開始、280 秒後に等速直線運動開始）

4．実験結果

レドーム内でスプーフィング信号を送信していない状況での実験結果を正常値、スプーフィング信号が送信された状況での実験結果をスプーフィング値として評価を行う。また、今回目標とするのは u-blox 受信機とする。実際に得られた経路を以下に示す。黒線がスプーフィング開始タイミングを表す。

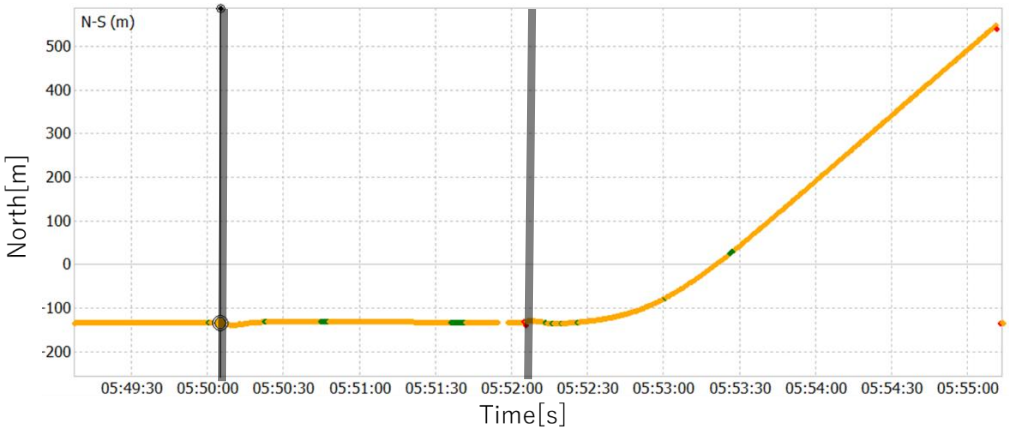

図 4　u-blox 受信機で取得した GPS の軌跡（南北方向）

図 3 と図 4 の軌跡がよく一致していることから、時刻同期スプーフィングが成功したと判断し、こちらのデータを用いて検知可能か検証を行う。以下では信号強度及び、観測残差に焦点を当てて説明を行う。黒線がスプーフィング開始タイミングを表す。

以下で、信号強度及び、観測残差を用いてスプーフィング検知を行う。まず信号強度について、スプーフィング環境での信号強度を以下の図 5 に示す。実信号のみの場合 25～45dB の範囲でばらつきをも分布していた信号強度がスプーフィング信号開始以降、全て 45db 付近の一定値に収束していることが分かる。つまり信号強度の標準偏差が極端に小さくなったことが分かる。このことより、実際のスプーフィング環境であっても信号強度の変動や各衛星の強度分布を監視することにより、スプーフィングを検知することは可能と考えられる。

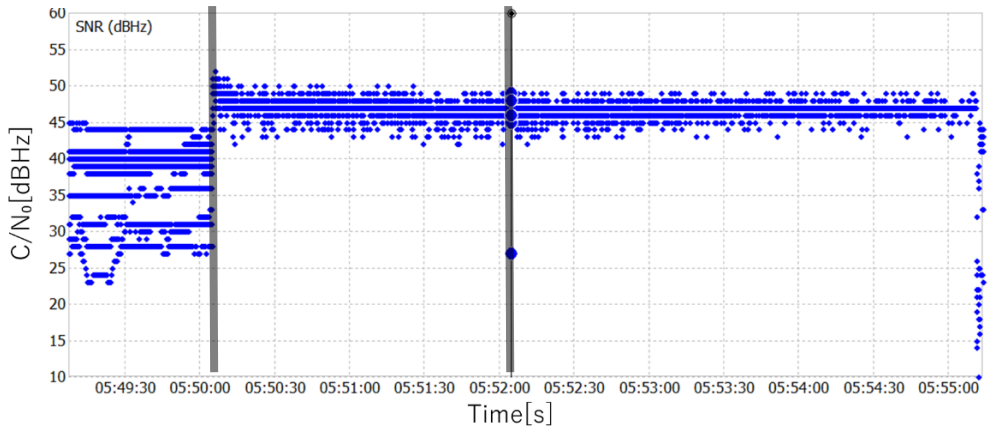

図 5　スプーフィング環境での信号強度（dBHz）

次に観測残差について、これは受信機で取得した擬似距離と、Tightly-coupled で得られた（加速度や角速度を時間積分し、GNSS で補正された）擬似距離の差を表す。スプーフィング信号の無い環境での G15 番衛星の観測残差を図 6 に、レドーム内でのスプーフィング環境での G14 番衛星の観測残差を図 7 に示す。黒線が静止スプーフィング開始タイミングを表す。

正常値の観測残差（左図）が 0 付近で一定値に収束していることが分かる。一方で、スプーフィング値（右図）はスプーフィング信号開始と同時に残差の値が大きくなりその後も数mのばらつきが生じていることが分かる。これは、スプーフィング開始時に強力な信号によって信号追尾のロックが外れ、信号の再捕捉が行われ、残差の再計算が行われるため大きく変化する。このことより、実際のスプーフィング環境であっても観測残差の平均値や標準偏差を監視することにより、スプーフィング信号の到来を検知することは可能と考えられる。

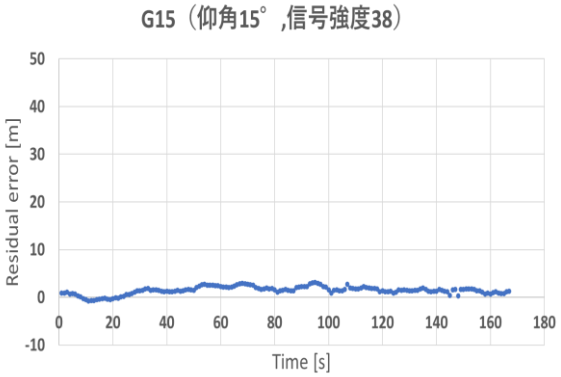

図 6　正常な環境での観測残差

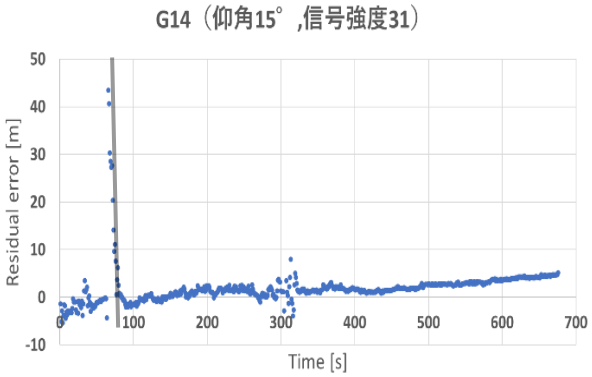

図 7　スプーフィング環境での観測残差

5．研究成果のまとめと今後の課題

以前に実施した非同期型スプーフィング実験により、信号強度の変動や観測残差の平均値などからスプーフィング信号の検知が可能であると推測された[4]。本研究では、同期型スプーファーを用いた実環境実験を行い、以上の 2 つの評価指標の有効性を検討した結果、実環境でもスプーフィング検知は可能であると分かった。

本実験で使用したスプーフィング設備では、GPS の実信号を受信し、GPS シミュレータを用いてスプーフィング信号を生成する際に実信号とタイムラグが発生してしまい、完全な時刻同期が行えていないことからスプーフィングできない状況も度々見られた。今後の課題として、信号捕捉の段階で時刻にどれ程のずれが生じているのか確認し補正を行うことが考えられる。また、様々な実験シナリオで、これらの評価指標が有効か検証する必要がある。さらに、スプーフィング検知のための新たな評価指標について検討を行う予定である。

参考文献

[1] Liu, Yang, Sihai Li, Qiangwen Fu, and Zhenbo Liu. 2018. "Impact Assessment of GNSS Spoofing Attacks onINS/GNSSIntegratedNavigationSystem" *Sensors* 18,no.5:1433. https://doi.org/10.3390/s18051433

[2] Blum, Ronny, Dütsch, Nikolas, Dampf, Jürgen, Pany, Thomas, "Time Synchronized Signal Generator GNSS Spoofing Attacks against COTS Receivers in over the Air Tests," *Proceedings of the 2021 International Technical Meeting of The Institute of Navigation*, January 2021, pp. 125-148. https://doi.org/10.33012/2021.17814

[3] Sharma, Himanshu, Bochkati, Mohamed, Pany, Thomas, "Time-Synchronized GNSS/IMU Data Logging from Android Smartphone and its Influence on the Positioning Accuracy," *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. 2000-2011.

[4] 塩谷秀登、“IMU との複合航法による GNSS スプーフィング検知に関する研究”第 60 回飛行機シンポジウム