GNSS/IMU 複合航法による GNSS スプーフィングの検知と除去

The research on GNSS spoofing detection and removal using GNSS/IMU integrated navigation

八杉尚樹　　辻井利昭
Naoki Yasugi　　Toshiaki Tsujii

大阪公立大学大学院
Graduate School of Engineering, Osaka Metropolitan University

１．研究テーマの背景・目的

全地球測位衛星システム (GNSS) スプーフィング攻撃とは，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，誤った位置や時刻情報を生成させることを指す．民間の GNSS サービスは，衛星信号がオープンであることと地表に到達するまでに減衰し低電力になる事から，スプーフィングに対して脆弱である．実際に，スプーフィングによってヨットの乗っ取りや航空機が 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．本研究では，スプーフィング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と除去を目的とする．

２．実験概要

本研究を進めるにあたり，Fig.1 の実験機器を構成し，移動体に対するスプーフィング実験を行った．対象の移動体には，IMU センサとして AsteRx-i3 (Septentrio)，GNSS 受信機として M8T (u-blox) を搭載し，測位を行った．偽の GPS 信号を bladeRF というソフトウェア無線機で生成した．屋外での偽信号の放射は法律による規制が厳しいため，GPS Combiner を経由し，有線で GNSS 受信機に送信した．

今回，対象の移動体は大学構内で直線運動を行った．実験は３つのフェーズで構成した．フェーズ１では，スプーフィング攻撃を行わずに 100m ほど直進した．フェーズ２では，スプーフィング攻撃により，実際の運動に近い経路偽装を受けながら，さらに直進した．フェーズ３では，スプーフィング攻撃により，実際の運動と異なって分かれ道で直角に曲がる経路偽装を受けながら，さらに直進した．Fig.2 に実験の様子を示した．

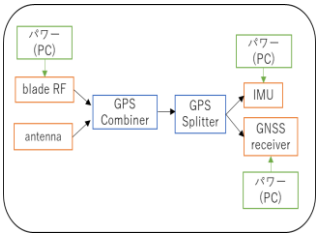

Fig. 1 実験機器の構成

Fig. 2 実験の様子

３．実験結果

計測データより，対象の移動体の測位結果を GNSS と IMU の複合航法演算プログラムである”Ninja”を使用して計算した．

Fig. 3 は GNSS 計測データから演算した測位結果である．スプーフィング攻撃により，対象に気づかせずに捕捉信号を実信号から偽信号へと入れ替え，実際の運動と異なった測位結果を出力していることから，対象は乗っ取られている．Fig. 4 は GNSS 計測データと IMU 計測データから，tightly coupled 複合方式で演算した測位結果である．捕捉信号が偽信号へと置き換わる際に，対象の測位結果は実際の位置と大きくずれている．測位結果の軌道は実際の運動の軌道と異なっていることから，対象は乗っ取られている．まとめると，GNSS スプーフィング攻撃への GNSS 測位の脆弱さについて，理論を実感できた．一方で，IMU により GNSS の脆弱性を補うことができておらず，理論の検証に至らなかった．

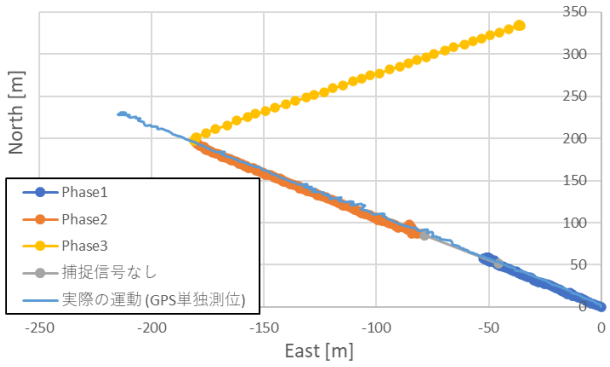

Fig. 3 GNSS による測位結果

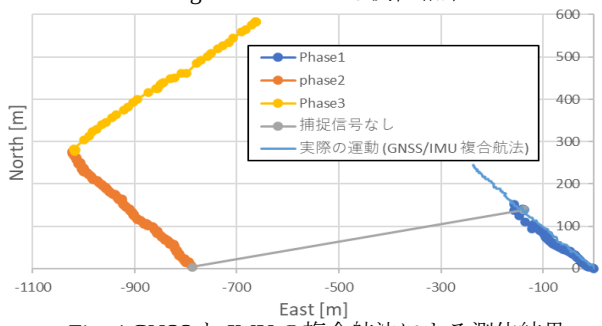

Fig. 4 GNSS と IMU の複合航法による測位結果

４．今後の課題

今回の実験では，偽信号の時刻情報が実信号のそれと数十秒レベルの誤差を持つため，高精度なスプーフィング実験は実施できなかった．今後は JAXA 様協力のもと，より高精度な GPS simulator を用いて，GNSS スプーフィング攻撃に対する GNSS/IMU 複合航法システムの冗長性を評価する予定である．

５．参考文献

(1) 海老沼拓史 bladeGPS
(https//github.com/osqzss/bladeGPS.)
(2) 成岡優 ninja-scan-light
(GitHub - fenrir-naru/ninja-scan-light.)