統合測位受信機を搭載した自動車に対するスプーフィング実験の報告

東京海洋大学
小林海斗、久保信明、鈴木翔

第6回SAPT研究発表講演会
2024/08/29

発表内容

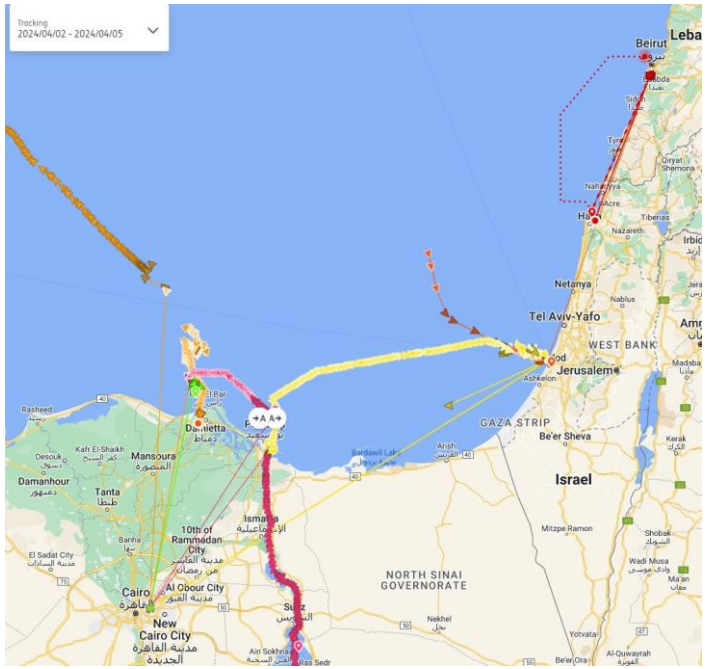
1. 背景
2. スプーフィング方法について
3. 実験構成
4. 実験結果
5. リピーター信号を使用した実験
6. 実験のまとめ

1. 背景

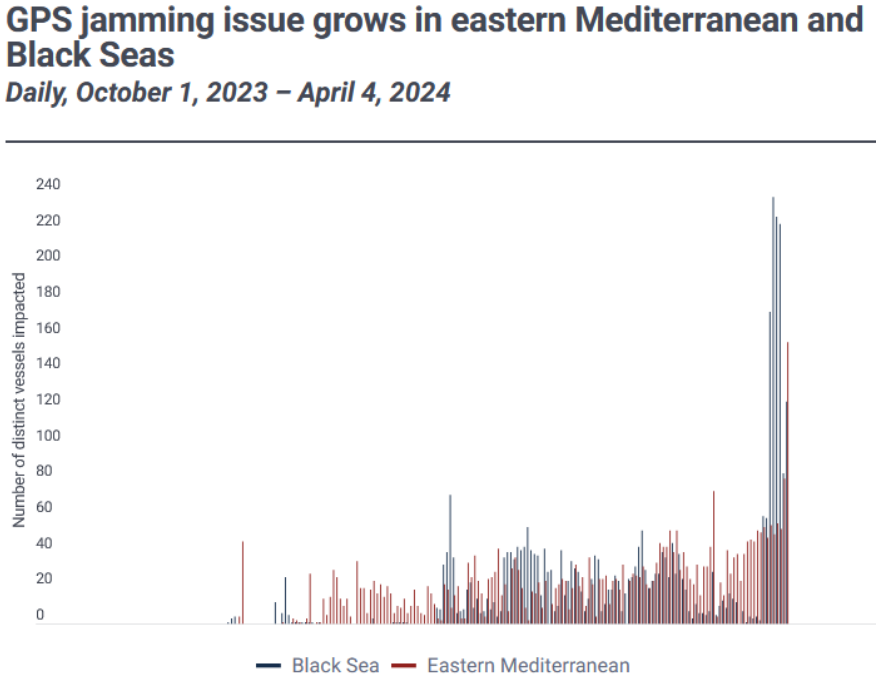
◆GNSS分野でのスプーフィング（なりすまし）やジャミングの頻度は国際情勢の悪化に伴い年々増加している。

◆これはGNSSを使用した移動体の無人制御などに大きな影響を及ぼす。

◆また紛争地域で行われているジャミング、スプーフィングはかなり大規模で被害範囲が広い。



スエズ運河付近で船の位置が
カイロやレバノンの空港に移動したデータ
(https://www.lloydslist.com/LL1148748/War-zone-GPS-jamming-sees-more-ships-show-up-at-airports)



ジャミング報告数の増加

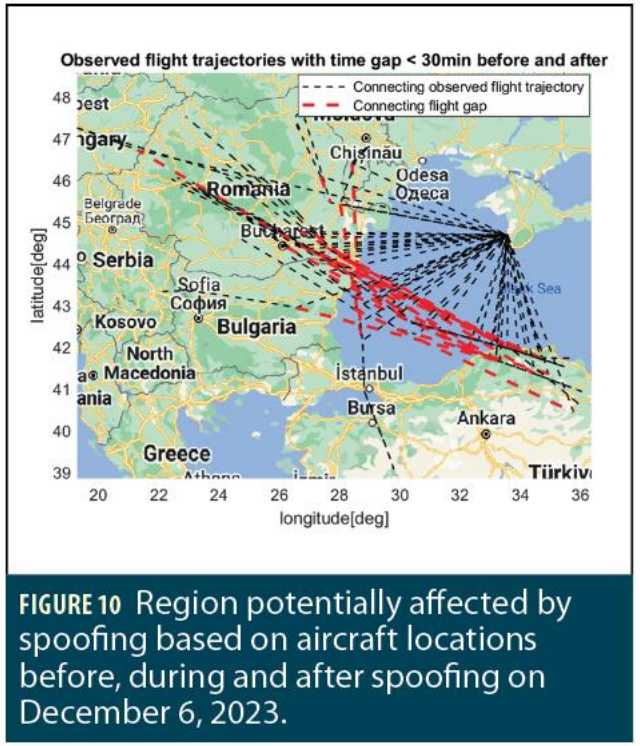


FIGURE 10 Region potentially affected by spoofing based on aircraft locations before, during and after spoofing on December 6, 2023.

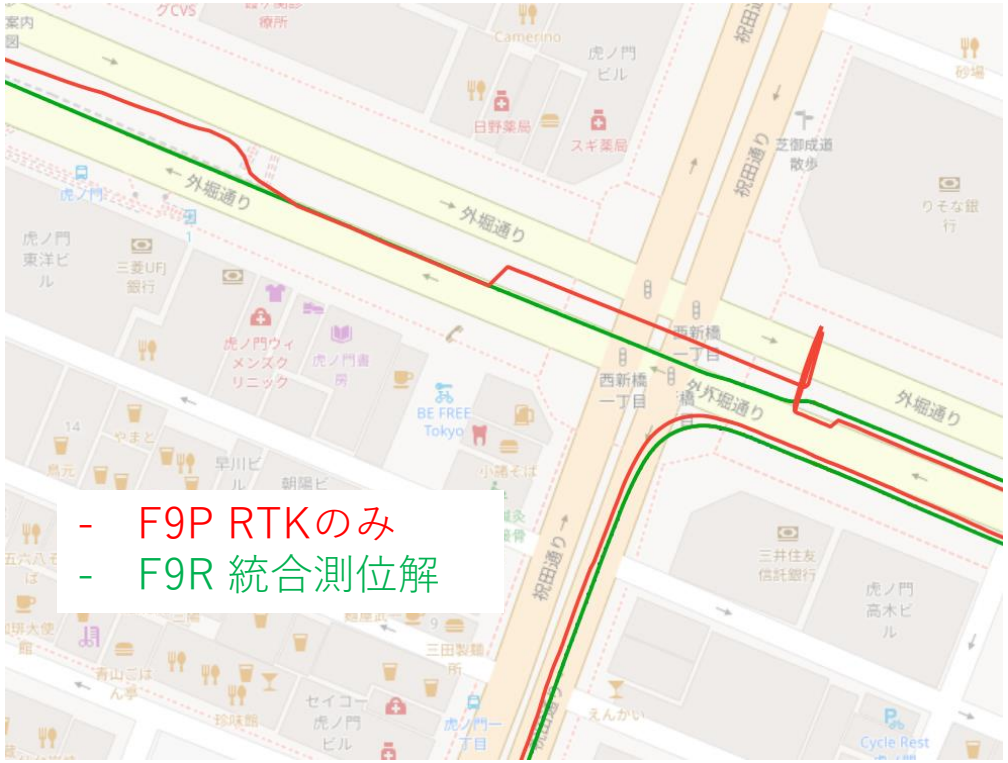
黒海上空でスプーフィングされる航空機
(https://insidegnss.com/gnss-spoofing-and-jamming-in-eastern-europe/)

1. 背景

◆自動車は高層ビル街、トンネルや高架下を通過するため、常にGNSSが観測できる航空機や船舶と異なり、通常IMU(慣性計測ユニット)や車速パルスをGNSSと組み合わせて位置決定が行われる。

◆これは自動運転用のハイエンド受信機だけではなくローコストなカーナビやスマホナビでも同じである。

◆今回走行中の車両を狙ったスプーフィング攻撃を想定して、実際に位置情報の乗っ取りが可能かを実験した。

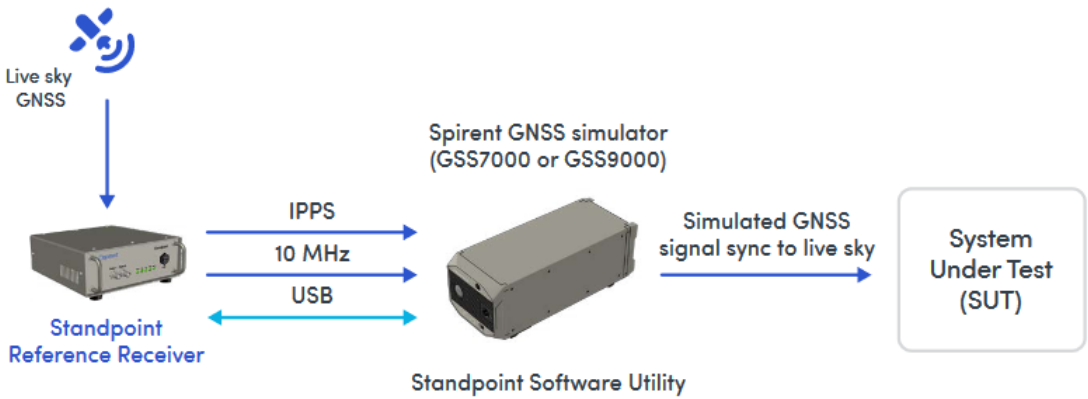


2. スプーフィング方法について

◆これまでのスプーフィング実験からスプーフィング信号とライブ信号で時刻とエフェメリスが一致しないとスプーフィングは難しいことがわかっている。

◆この条件を満たさずにスプーフィングする場合
・スプーフィングの信号強度をライブ信号よりも遥かに強くする
・ジャミングで一度対象受信機の信号追尾を切る
・長時間スプーフィングし続ける。
必要がある。

◆2024年3月に暗室でシミュレーターからの信号をライブ信号と時刻同期させるSpirent Stand Pointを使用して実験を行った。この実験ではスプーフィング信号、ライブ信号ともにGPS L1信号のみを使用したがライブ信号よりも5~10dB強いスプーフィング信号でublox F9Pおよびseptentrio mosaic x-5を10~20秒ほどでスプーフィングすることができた。



2. スプーフィング方法について

◆しかし3月の実験では静止した受信機に対して、同じ位置で3分スプーフィングしてから乗っ取るという条件であった。

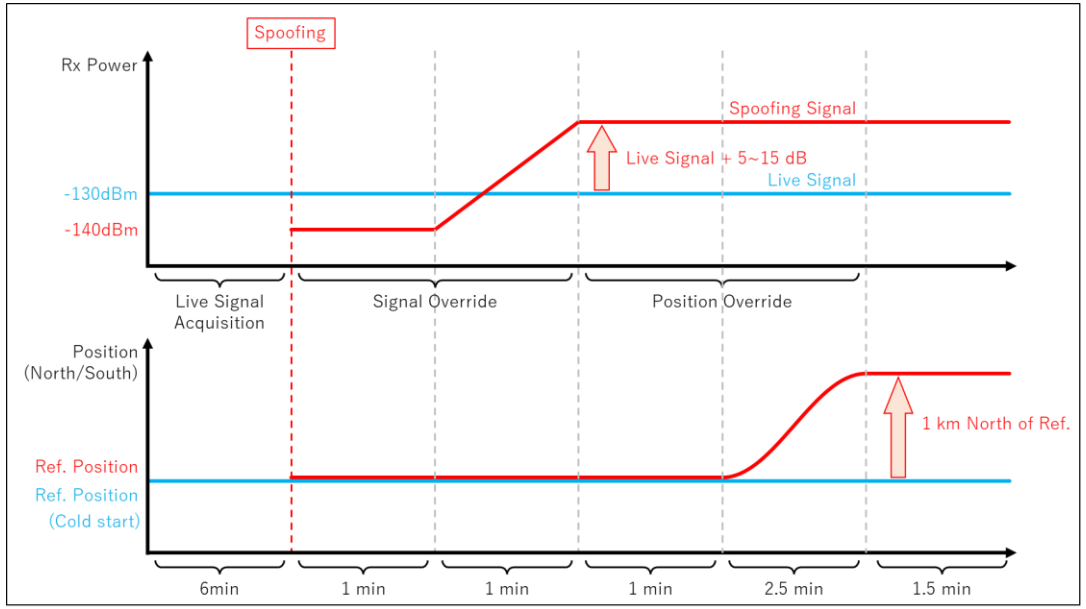
◆これを移動体へのスプーフィングに適用する場合、相手の位置を知り、リアルタイムでスプーフィング位置を対象の座標に移動する必要がある。

◆船舶はAIS、航空機はADS-Bで自分の位置を送信しているが精度は単独測位の精度。

◆自動車は将来的にV2Xなどで自車位置を送信するかもしれないが、今現在は送信していない。

◆今回もStand PointとGSS7000シミュレーターを用いて移動中のIMU＋GNSS搭載の自動車を対象とし、大体の位置でスプーフィングを試みる。

暗室内静止状態実験のシナリオ



2. スプーフィング方法について

◆福島ロボットテストフィールドにて実験を行う。

◆長方形の道路を車で周回。

◆車の移動に沿って北東方向にそれぞれ10mずらした位置を設定する。

◆車は南西角から出発。15km/hで走行。1周83秒。

◆Stand Pointをスタートしてから実際に電波が出るまで60秒のシンクロ時間があるので、スプーフィングは60秒走った位置から開始する。その後15km/hで移動。

◆その後乗っ取りがされるまで周回を続ける。

◆有線でスプーフィングを行うのでGPS, GLONASS, Galileo, BDS, QZSSのマルチGNSSかつL1/L2/L5帯の3周波で信号を生成した。

3. 実験構成

◆実験日 2024/06/20 9:00-16:00

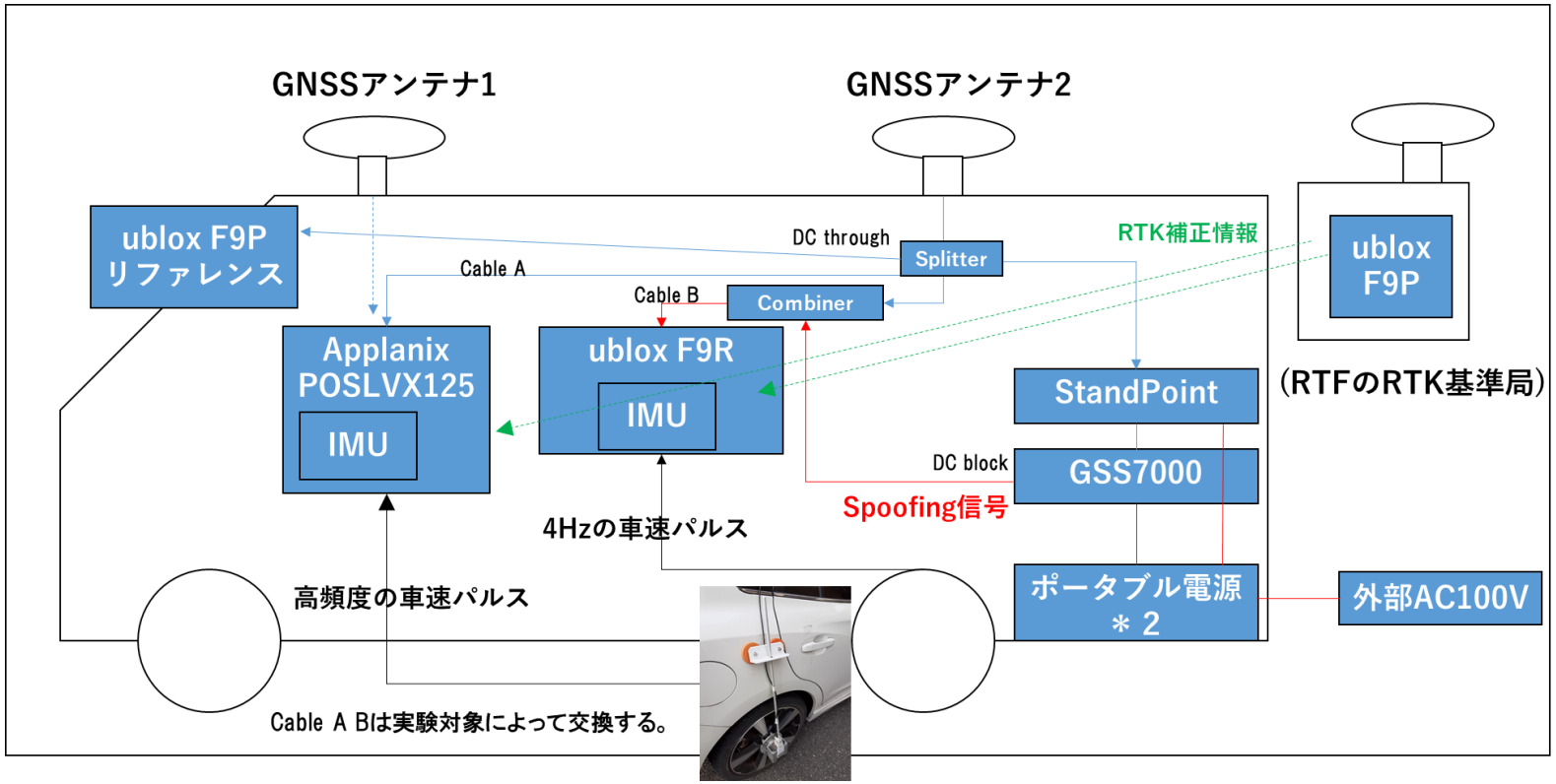
◆海洋大としては車載のIMU、速度センサー付き市販GNSS受信機をSpoofingして統合測位解がどうなるかを検証したい。

◆対象受信機

・Applanix POSLVX125（ハイエンド）
・ublox F9R（ローコスト）
・リファレンスとしてublox F9P

◆Spoofing信号はStandPointとGSS7000でGNSSアンテナ2と時刻同期したものを作る。

◆StandPointとGSS7000(500W)は車両に搭載しポータブル電源から給電。



3. 実験構成

◆使用した統合測位受信機について

	ublox F9R	Applanix POSLVX-125
GPS	L1/L2	L1/L2/L5
GLONASS	G1/G2	G1/G2
BDS	B1I/B2I	B1I/B1C/B2I/B2a
Galileo	E1C/E5b	E1C/E5a/E5b
QZSS	L1/L2	L1/L2/L5
IMU	内蔵MEMS	内蔵MEMS
車速パルス	車載標準4Hz	専用高頻度
方位	-	GNSSコンパス

DMI: POS LV に標準装備された測距インジケータ (DMI) は、ホイール式回転シャフトエンコーダで、移動した直線距離を正確に測定し、GNSS 信号停止によるドリフトを抑制する効果があります。

3. 実験構成

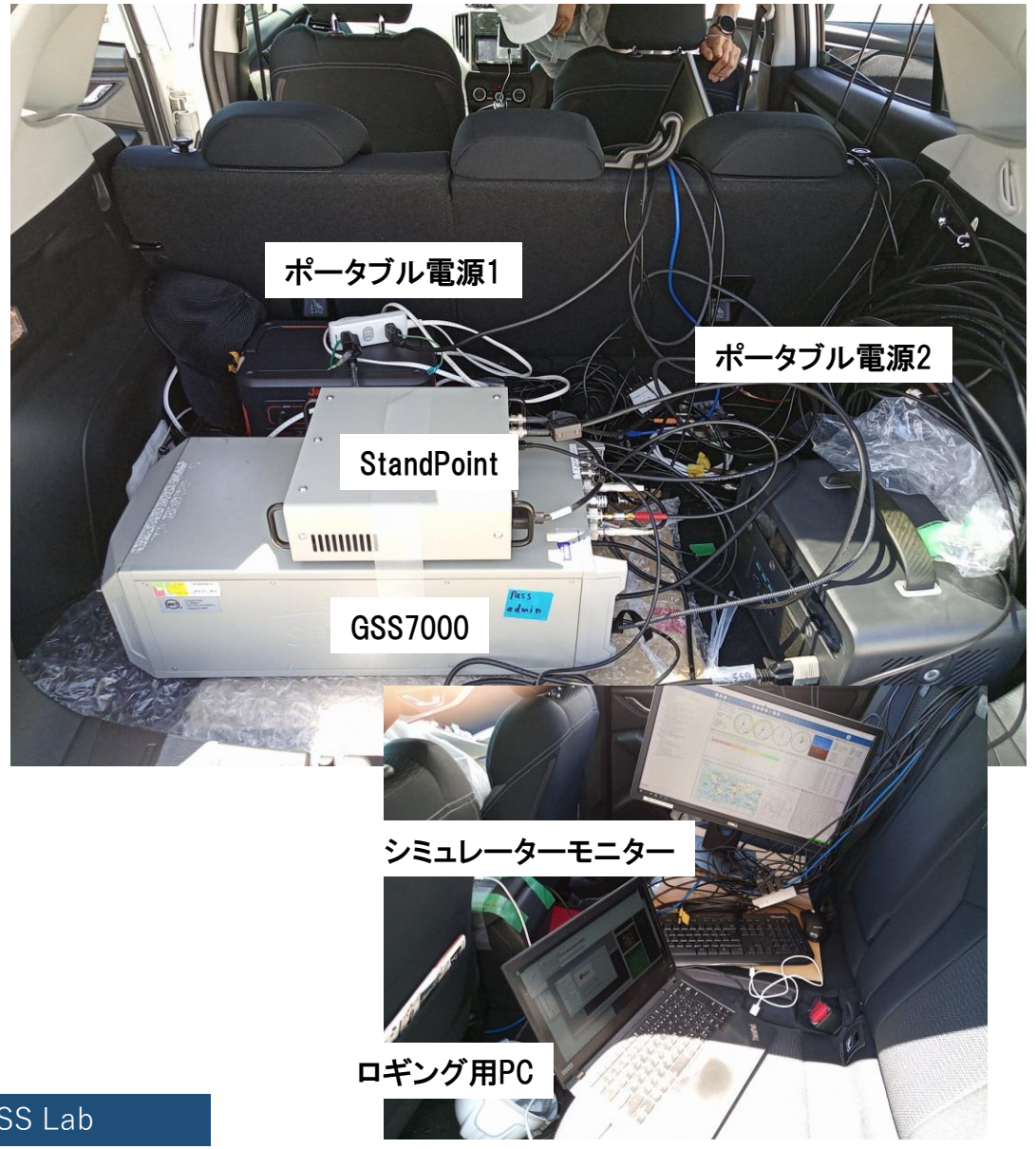
◆車のトランクにGSS7000とStandPointを置く。

◆ポータブル電源1はStandPoint, POSLVX, 液晶用。

◆ポータブル電源2はGSS7000用。

◆受信機、モニター、キーボード、ロギング用PCは後部座席に置く。

◆RTK基準局は事前に真値を決定し、LTEでNTRIPサーバーへRTCMを送信。



4. 実験結果

◆走行実験はSpoofing信号、ライブ信号の電力を変更して3回実験をした。

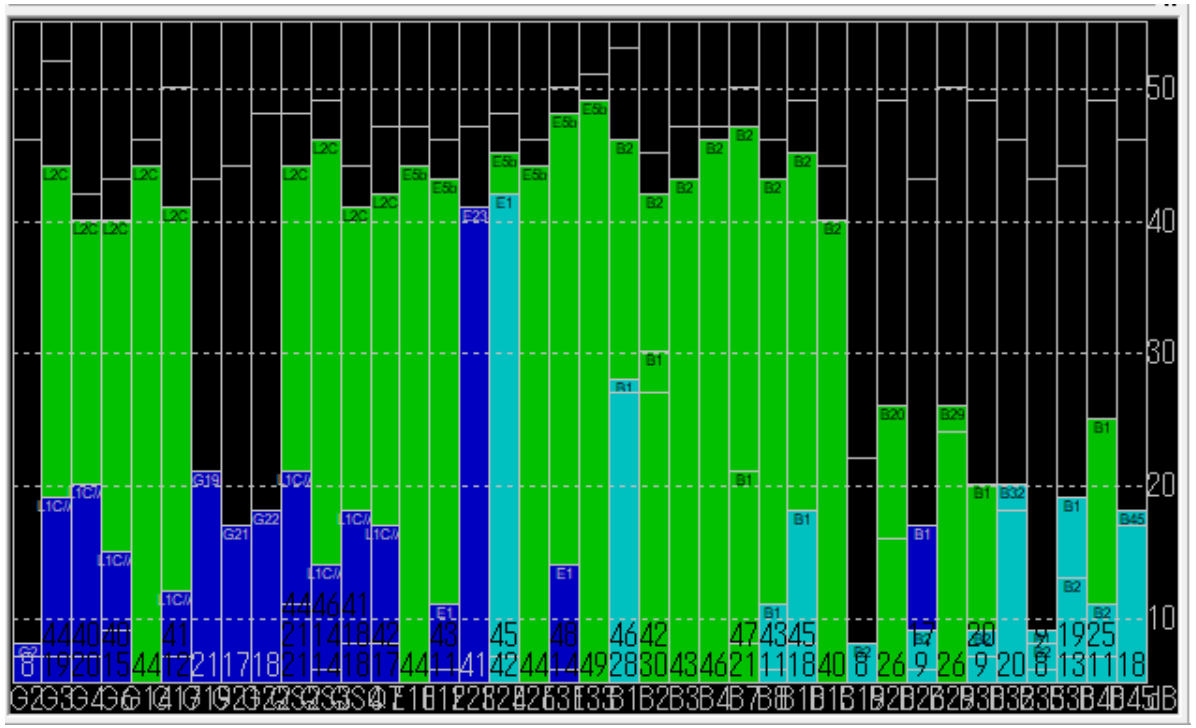
◆s2、スプーフィング信号：-70dBm

◆s2b、スプーフィング信号を-65dBmに変更

◆s2c、さらにライブ信号をアッテネーターで10dB減衰

◆s2cでようやくF9Rでスプーフィング信号を確認できた。

◆以降s2cの結果について分析する。



青（捕捉）、水色（追尾）がスプーフィング信号

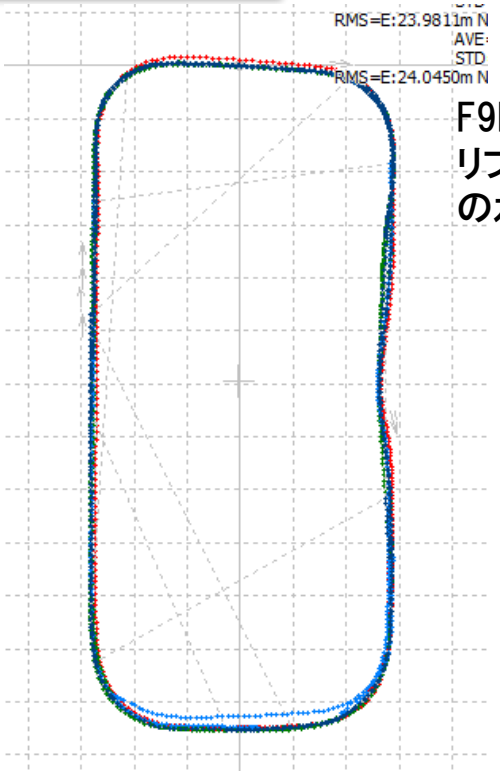
4. 実験結果　F9R

◆結論としてPOSLVX125, F9Rともに乗っ取りはされなかった。

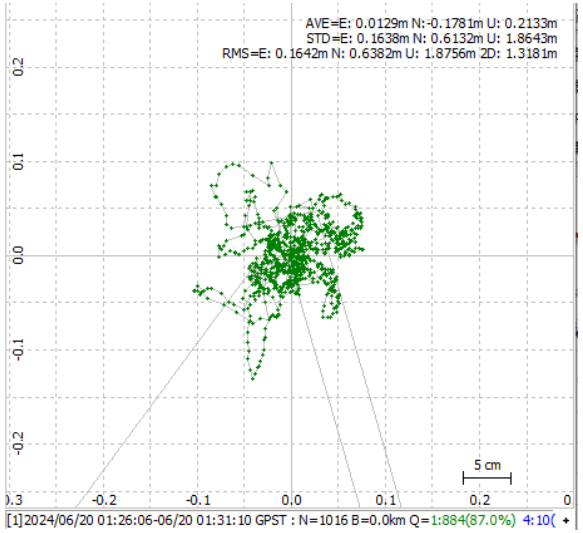
◆Spoofing開始時刻はtow=350766（01:26:06)

◆F9RはSpoofing Indicatedの表示が出て、スプーフィング信号を測位に使用せず、ライブ信号を追尾して測位を継続させた。

◆もちろん測位結果の座標はずれなかった。

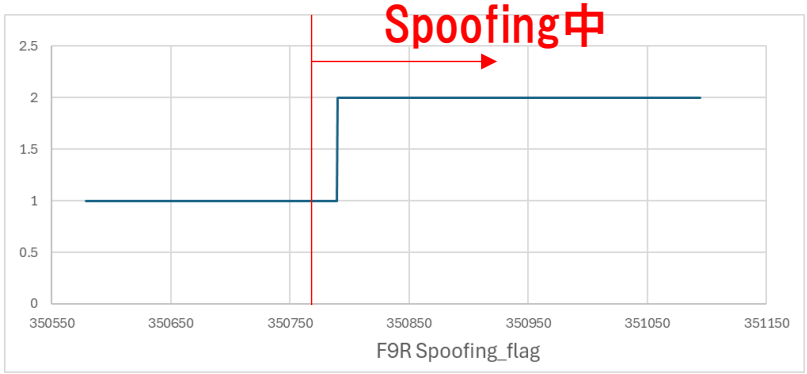


F9Rと
リファレンスF9P
の水平プロット



UBX - NAV (Navigation) - STATUS (Navigation Status)　5 s

Param	Value
Position Fix Type	3D+DR
Position within Limits (FixOK)	Yes
DGNSS Fix	Yes
Weeknumber Valid	Yes
Time of Week Valid	Yes
Diff Corrections Available	Yes
Map Matching	None
TTFF	21.480 s
Time since Powerup	4133.081 s
PSM state	ACQUISITION
Spoofing detection state	SPOOFING INDICATED
Carrier Range Status	Fixed



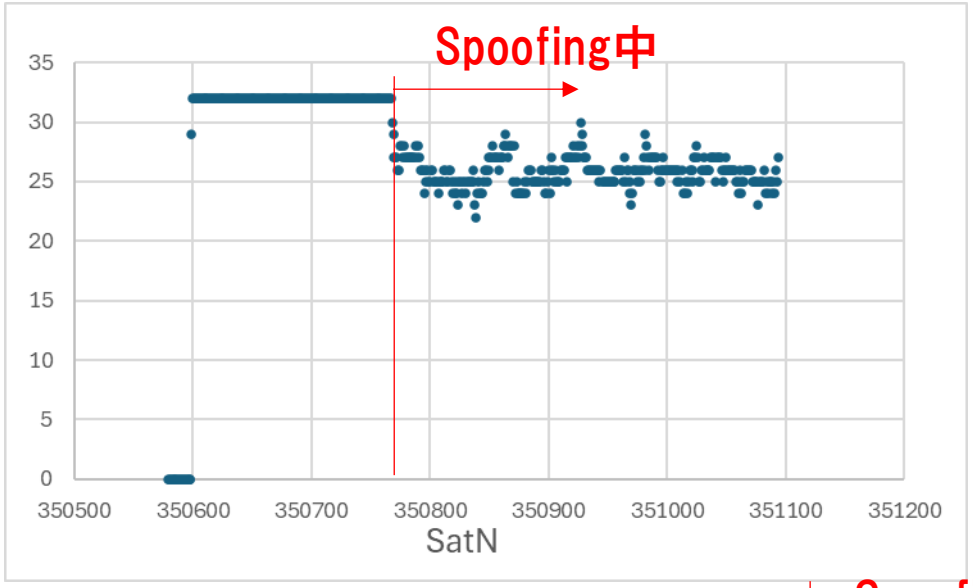
Spoofing後のF9Rの精度は
F9Pに比べて10cm以内
→Spoofing信号が入っても悪化していない

4. 実験結果　F9R

◆F9Rの利用衛星数はSpoofingによって6~8基ほど減少。

◆今回はオープンスカイ環境でもともと衛星の数は多かった。

◆信号強度についてはスプーフィング時に30dBほどまで大きく減少し、25秒後からRINEXへの変換ができなかった。
（.ubxファイルにはRAWXパケットがあるのでRTKLIBの変換で削除されている？）



RINEXへの変換ができなかった

4. 実験結果　F9R

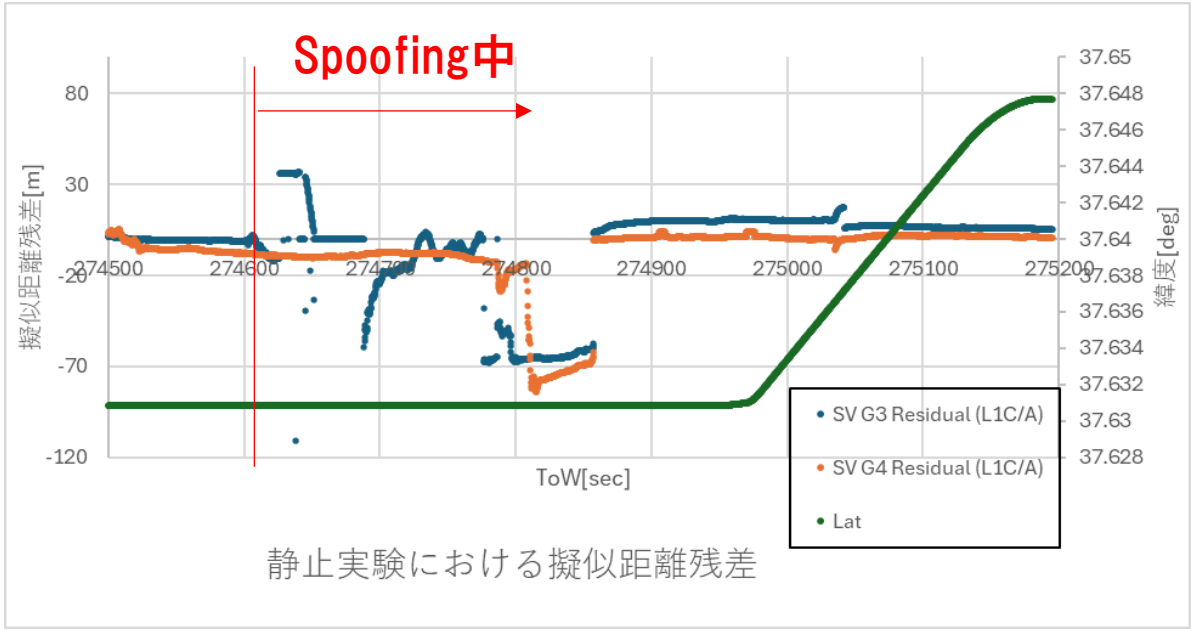
RAIMによるスプーフィング信号の排除

◆Stand Pointの時刻同期精度は公称50nsであるが実際の擬似距離残差には50ns以上の遅延が認められた。

◆F9PをGPSのみ受信する設定にして静止状態でスプーフィングしたときに最大70m(=230ns)ほどの擬似距離残差が発生した。

◆完全に乗っ取りがされると大きな擬似距離残差はなくなる。

SV	CN0	Residual	Nav	Qi	El	Az	Orbit	Healthy	DGN...	Co...	Corr...	EPH	ALM	AOP	ANO
G3	43	-61.30	N	7	7	56	EPH	Y	N	No...		Y	Y	N	N
G4	46	-69.50	N	7	33	53	EPH	Y	N	No...		Y	Y	N	N
G5	0	0.00	N	1	1	247	ALM	Y	N	No...		N	Y	N	N
G6	48	0.10	Y	6	69	3	EPH	Y	Y	R...	PR	Y	Y	N	N
G7	0	0.00	N	1	2	132	EPH	Y	N	No...		Y	Y	N	N
G9	47	0.10	Y	5	59	101	EPH	Y	Y	R...	PR+...	Y	Y	N	N
G11	48	-49.10	Y	7	37	306	EPH	Y	Y	R...	PR+...	Y	Y	N	N
G12	48	-33.50	Y	7	14	294	EPH	Y	N	No...		Y	Y	N	N
G17	48	0.90	Y	4	42	166	EPH	Y	Y	R...	PR	Y	Y	N	N
G19	38	-78.40	N	6	65	187	EPH	Y	N	No...		Y	Y	N	N
G20	41	-40.90	Y	7	25	260	EPH	Y	Y	R...	PR+...	Y	Y	N	N
G22	0	0.00	N	1	3	201	EPH	Y	N	No...		Y	Y	N	N
G25	0	0.00	N	1	2	320	EPH	Y	N	No...		Y	Y	N	N



静止実験における擬似距離残差

静止実験

4. 実験結果　F9R

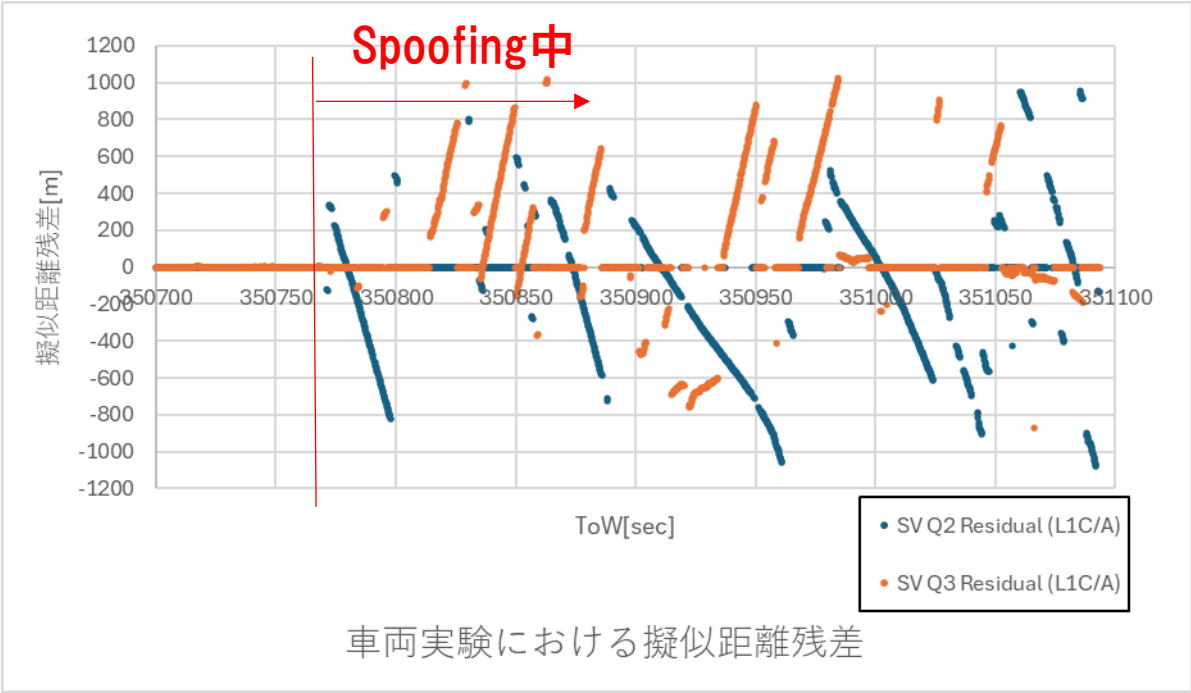
RAIMによるスプーフィング信号の排除

◆車両実験においてはSpoofing中の擬似距離残差は最大1km程度存在した。900mで時刻遅延は約3μs。

◆また静止実験と比べて時間による擬似距離残差の変化が大きい。

◆そのため、この擬似距離残差はスプーフィング信号の位置と実際の車両位置が移動しているためだと考えられる。

QS2	L1C/A	-	21	-739.80m	N	N	N	3	Y	None
QS2	L2CL	-	45	-1.60m	N	N	Y	7	Y	GPS
QS3	L1C/A	-	20	304.70m	N	N	N	4	Y	None
QS3	L2CL	-	46	-0.60m	N	N	Y	7	Y	GPS
QS4	L1C/A	-	21	-452.00m	N	N	N	4	Y	None
QS4	L2CL	-	41	0.10m	N	N	Y	7	Y	GPS
Q7	L1C/A	-	20	231.40m	N	N	N	3	Y	None
Q7	L2CL	-	43	-1.30m	N	N	Y	7	Y	GPS



車両実験における擬似距離残差

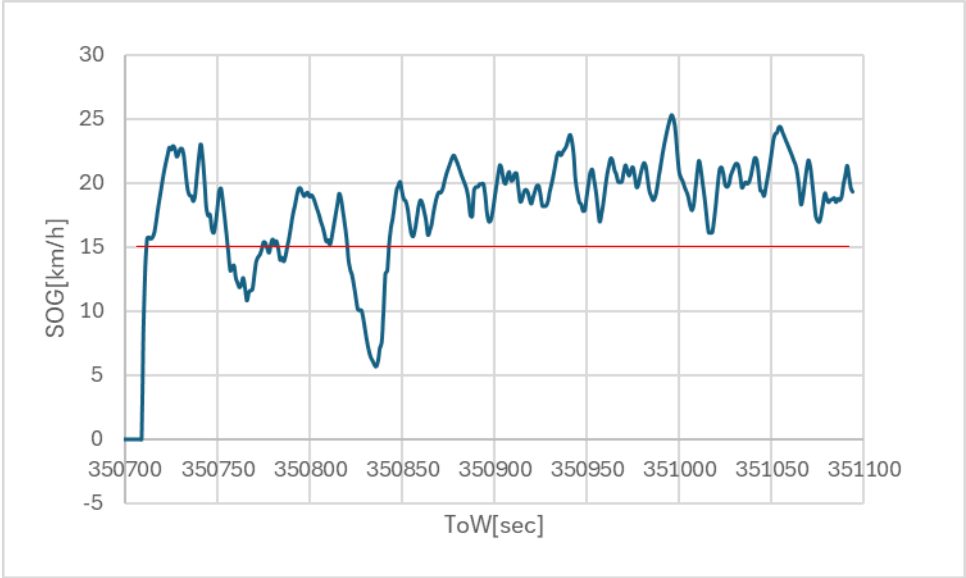
車両実験

4. 実験結果　F9R

◆実際の車両速度は全体的にSpoofingシナリオで設定した15km/hを超えていた。
→スプーフィング位置と車両位置の差が時間が経つにつれ開いていく。

◆スプーフィング開始時の位置は車の位置と18.9mずれていた。

◆スプーフィング信号と実際の車の速度も差があるのでスプーフィング位置と実際の車の位置の距離は時間が経つにつれて18.9mより増加。これが擬似距離残差の増加につながった可能性がある。

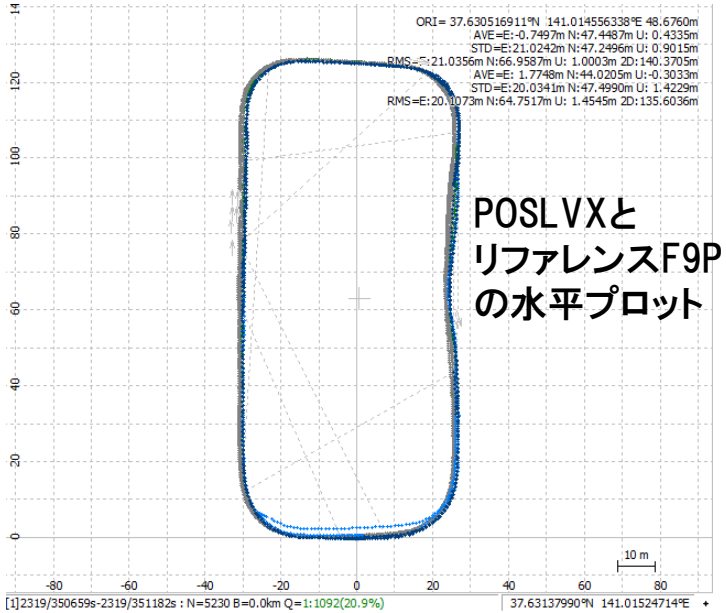


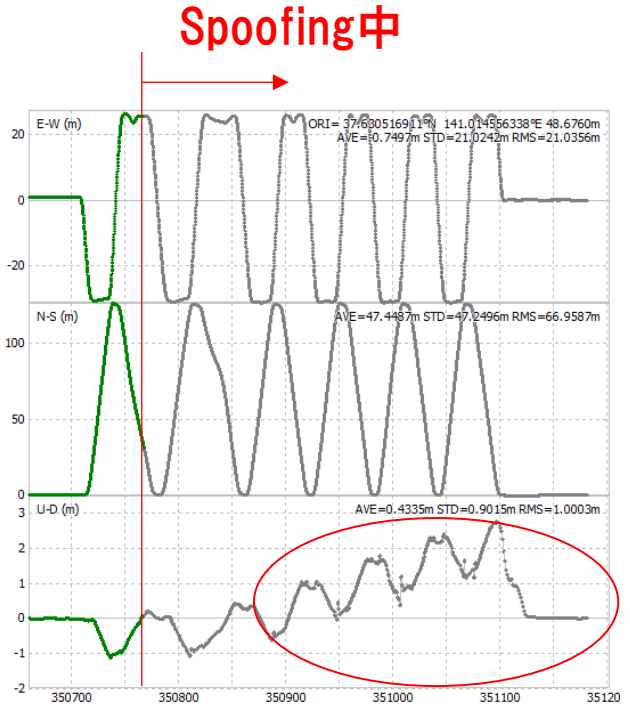
4. 実験結果　POSLVX125

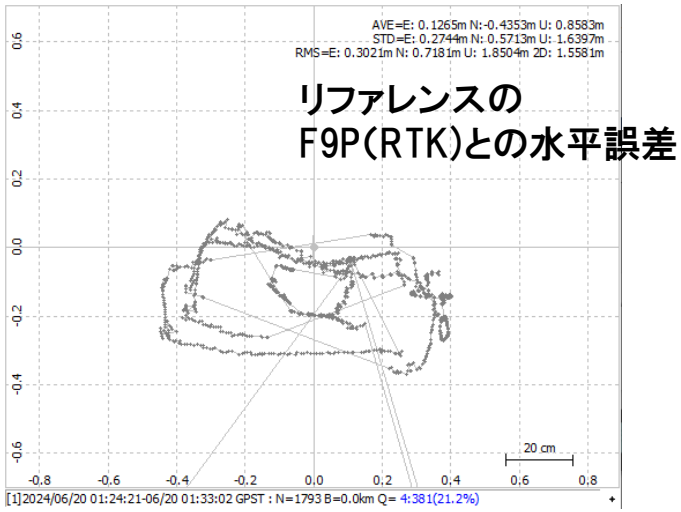
◆POSLVX125もスプーフィングによって乗っ取りはされなかった。

◆しかしF9Rと異なりGNSS測位を完全に諦めIMU、車速のみを使用したデッドレコニングに即座に切り替わった（グレー部分）。

◆デッドレコニングの結果は40cmほどの誤差と南方に20cmほどのバイアスがあった。また時間が経つにつれて高度方向の誤差が2.5mまで上昇した。（IMUの蓄積誤差）





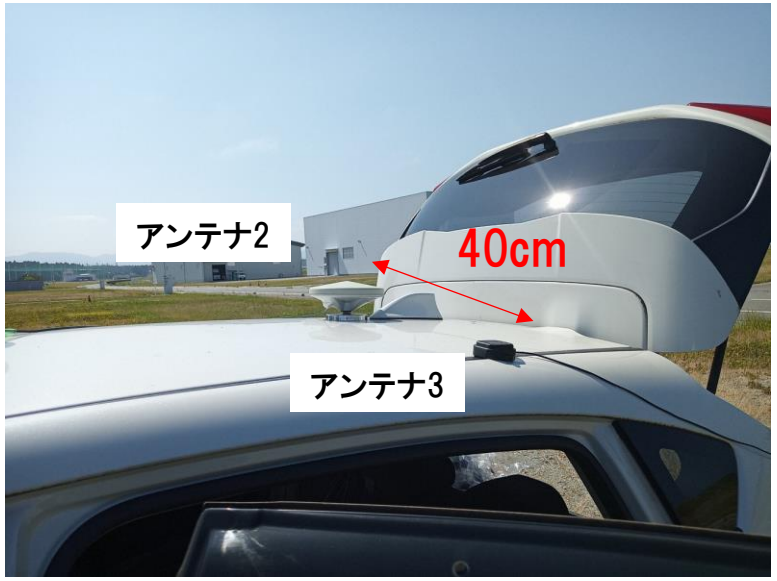


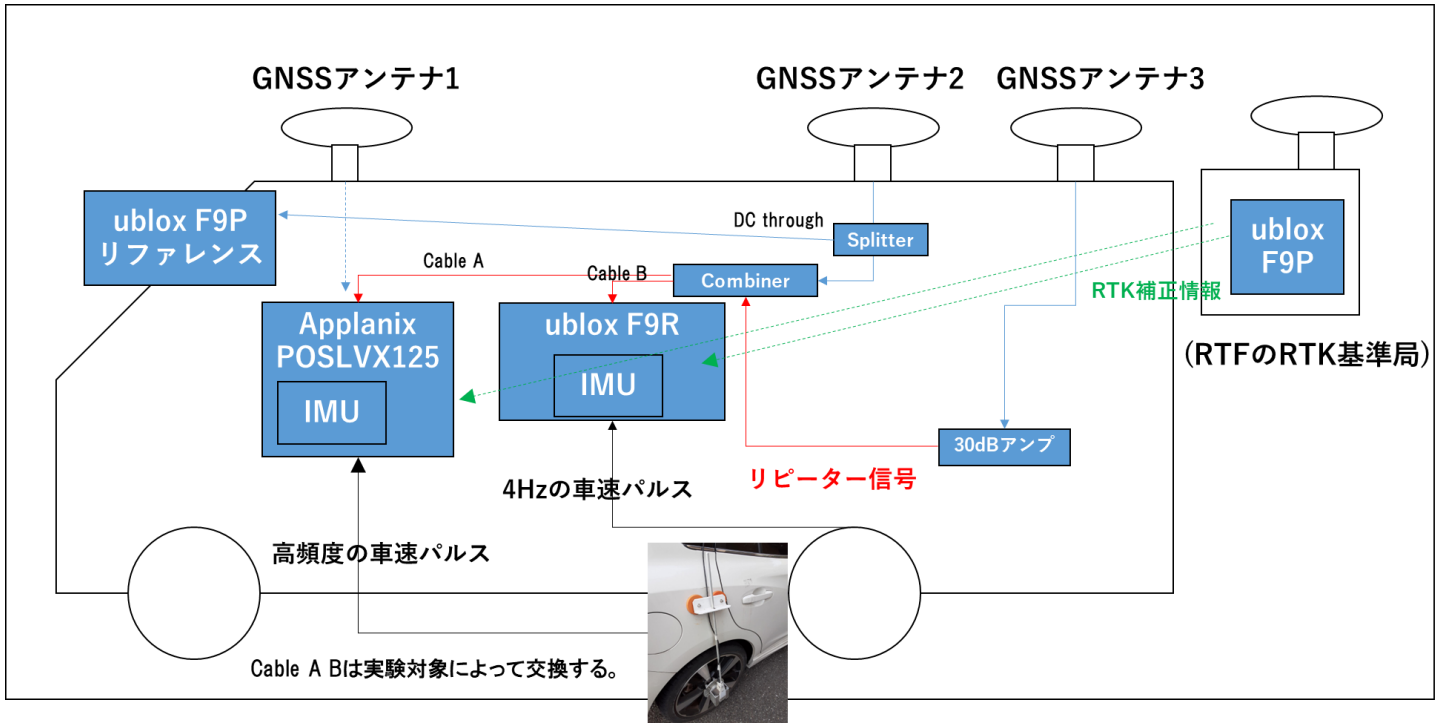
5. リピーター信号を使用した実験

◆シミュレーターで作成した信号でうまくスプーフィングができなかったため、別のアンテナ3からの信号をアンテナ2の信号に混ぜる実験を行った。

◆アンテナ3の信号はアンテナ2の信号より30dB高く設定した。

◆リピーター信号は時刻遅延が0秒。





5. リピーター信号を使用した実験

以下の順序で実験を行った。

1. アンテナ2のみで受信機のキャリブレーションをする。
2. 車両を停止してアンテナ3からのリピーター信号を追加。
3. リピーター信号を追加した状態で車両を南北方向に往復させる。

◆対象受信機はF9RとPOSLVX-125。

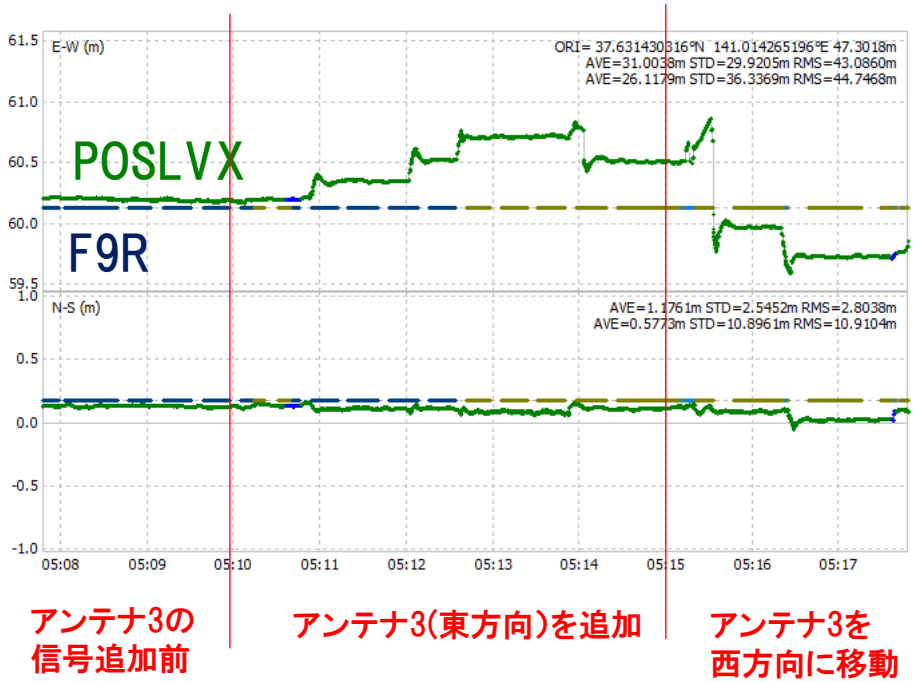
5. リピーター信号を使用した実験

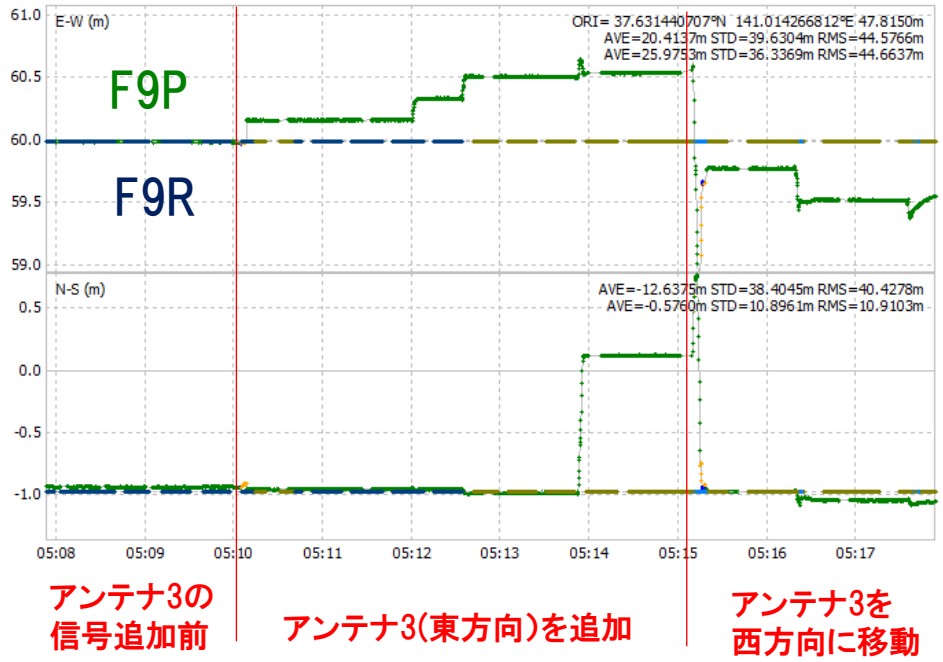
◆静止中にリピーター信号を加えたとき

◆F9Rの測位解は移動しなかった。

◆F9P(IMUなし)の測位解はリピーターアンテナの位置に従って移動した。

◆POSLVXの測位解はリピーターアンテナの位置に引っ張られたがF9Pと比べると移動に遅れがあった。

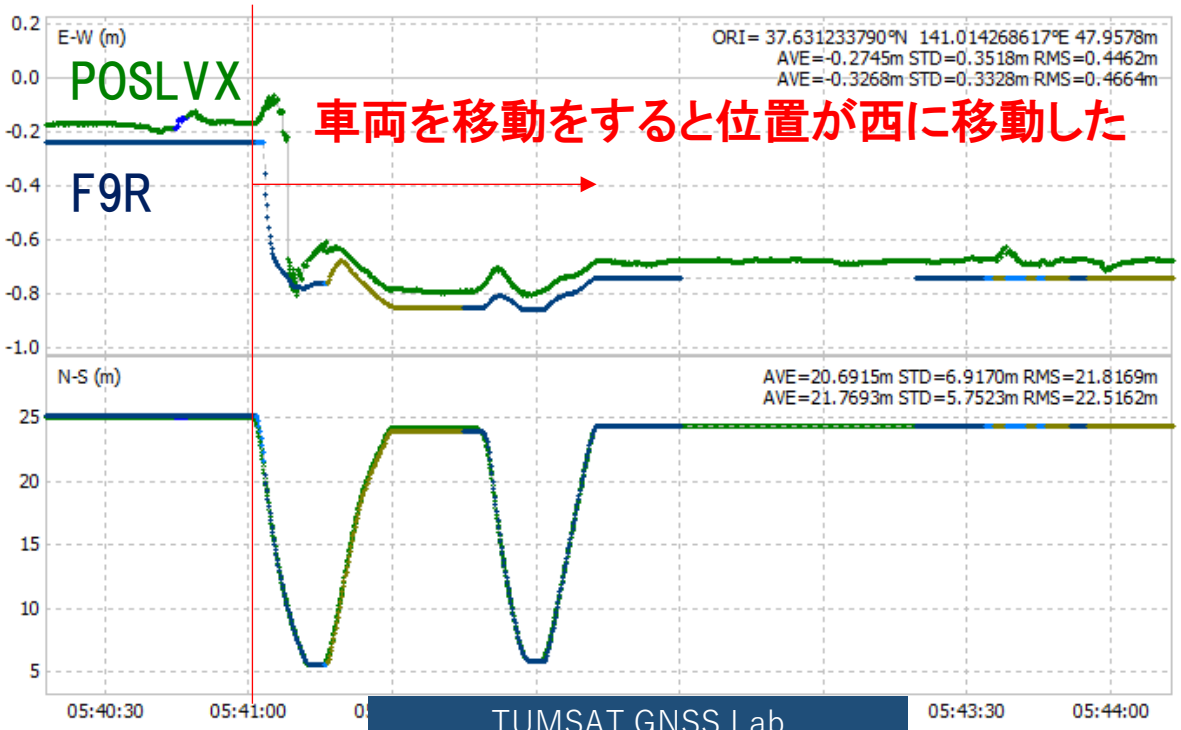




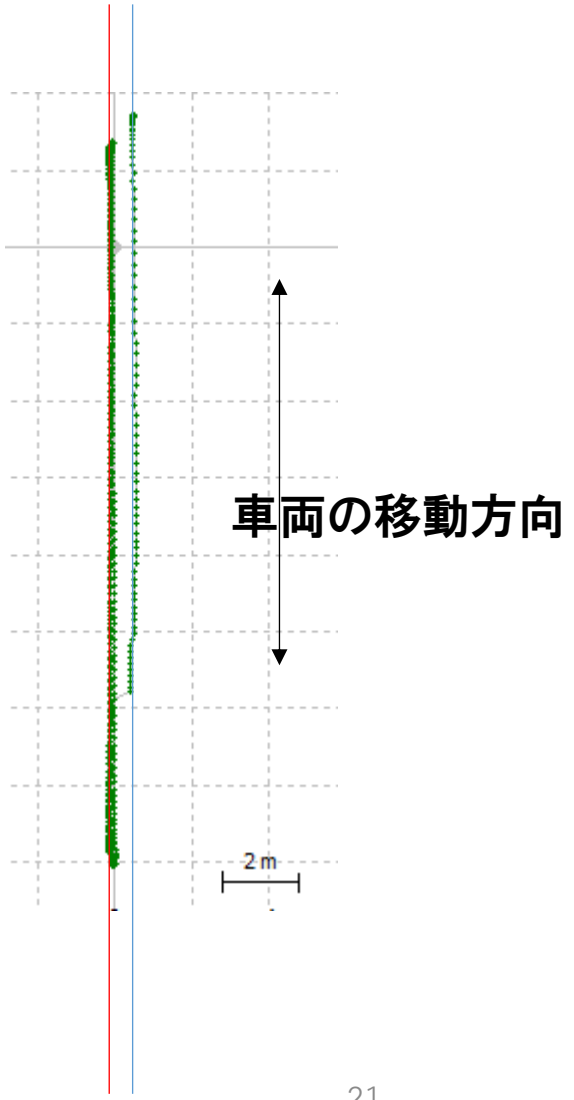
5. リピーター信号を使用した実験

◆静止中はIMUと車速パルスの拘束で測位解は移動しなかったF9Rだったが、車両を移動させるとリピーターアンテナの位置に乗っ取られた。

◆IMUと車速パルスの変化があるとスプーフィングに弱くなる。



リピーターアンテナの位置　　実際の車両位置



6. 実験のまとめ

◆移動体に対するスプーフィングは時刻同期スプーフィングであっても相手の位置と速度ベクトルにスプーフィングシナリオが一致しないと困難。リアルタイムに相手の位置と速度ベクトルを知る必要があるので静止体に対するスプーフィングよりも難しい。

◆StandPoint+GSS7000でもスプーフィング座標を外部から入力した座標（相手の位置）にリアルタイムに合わせることができないので、特定の相手の位置に合わせたスプーフィングは難易度、コスト面でパフォーマンスが悪い。

◆今回試した受信機POSLVX-125とF9RはGNSSよりもIMU＋車速センサーを信頼する設計になっていた。

◆特にF9Rは停止時に時刻遅延なしのスプーフィングを行っても位置が全く動かなかった。

◆しかし現実にスプーフィング被害は発生しており、これらは高出力信号とジャミングの併用が考えられる。また飛行機や船舶設置のGNSS受信機は古いものが多い。そのためAGCと信号強度のモニタリングなどの簡易的で低コストのスプーフィング検知手法を普及させる必要がある。

◆研究室で開発している統合測位アルゴリズムに対してスプーフィング結果がどのようになるか今後調査しスプーフィング排除アルゴリズムを明確にする。

◆本Spoofing Testは測位航法学会『Jamming/Spoofing勉強会』参加各機関の協力のもと行われました。Team Spoofing Test@福島RTF June 2024 by IPNTJ

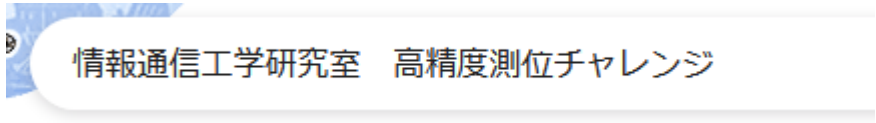
高精度測位チャレンジの紹介

◆今年も測位アルゴリズムを競う
高精度測位チャレンジを開催します。

◆参加期間は9~10月になります。
サイトのオープンまでしばらく
お待ち下さい。

◆上位3名に賞金が出ます。

検索



東京海洋大学 海洋工学部 海事システム工学科 GPS/GNSS 研究室

GPS/GNS

情報通信工学研究室

ホーム　研究紹介　メンバー　研究業績　調査　アクセス・連絡先　リンク　GNSS TUTOR　高精度測位チャレンジ

高精度測位チャレンジ（2024年度の予定）

今年度は第2回となる測位チャレンジを実施予定です。名城大学の目黒先生、千葉工大の鈴木先生の計3名の
スタッフで運営します。8月中にはデータを公開し、9月か10月頃まで参加者に評価頂き、
10−11月頃の測位航法学会のシンポジウムまたは別のオンライン等の会議で表彰を行う予定です。
今年度は鈴木先生がKaggleベースのコンテストサイトを作成されており、
Google Smartphone Decimeter Challengeと同じような参加形態になる予定です。
スポンサーとしてアイサンテクノロジー株式会社（https://www.aisantec.co.jp/）にご協力頂くこととなりました。
アイサンテクノロジー社は測量、モービルマッピングシステム、3D地図整備、自動運転に関するコンサルティングを
行っている企業で、GNSSと深い関連のある企業です。去年度と同様に上位3名まで賞金を出せる予定です。
データはGNSS受信機として廉価で定評のあるものを利用します。
また同時に取得したIMUのデータを取得し利用いただけるようにします。
データ取得場所は、去年と同じく東京都内と愛知県の名古屋となります。
データ公開までしばらくお待ちください。

去年度の開催に際して取得した、同コースのu-boxのF9PとPOSLVのレファレンス結果を以下に公開します。
u-bloxのF9Pの結果は前と後ろのアンテナの2つあるものもあります。今年度はもう少し短いコースに
する予定ですが、走行環境は同様のものにする予定です。都市部での測位精度向上の研究に
ご利用いただけると大変嬉しいです。