2つのアンテナを用いた GNSSスプーフィング検知手法の研究

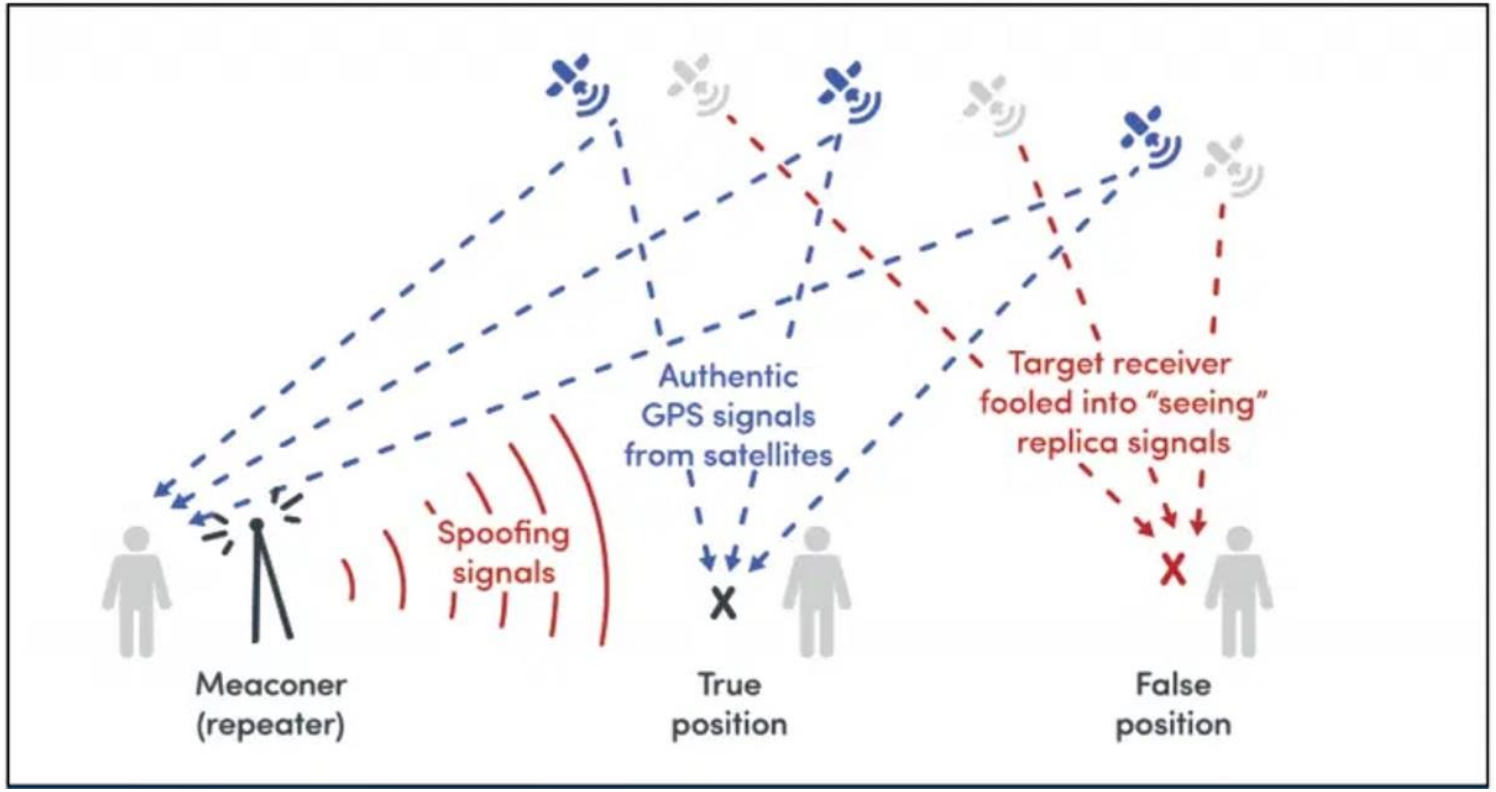
海運ロジスティクス専攻　2155014　長岡賢吾
指導教員　久保信明

目次

1. 研究背景
2. 信号到来方向監視による防御方法
3. 本研究の目的
4. 基線長解析による検知方法
5. 実験1
6. 実験2
7. 結果・考察
8. まとめ

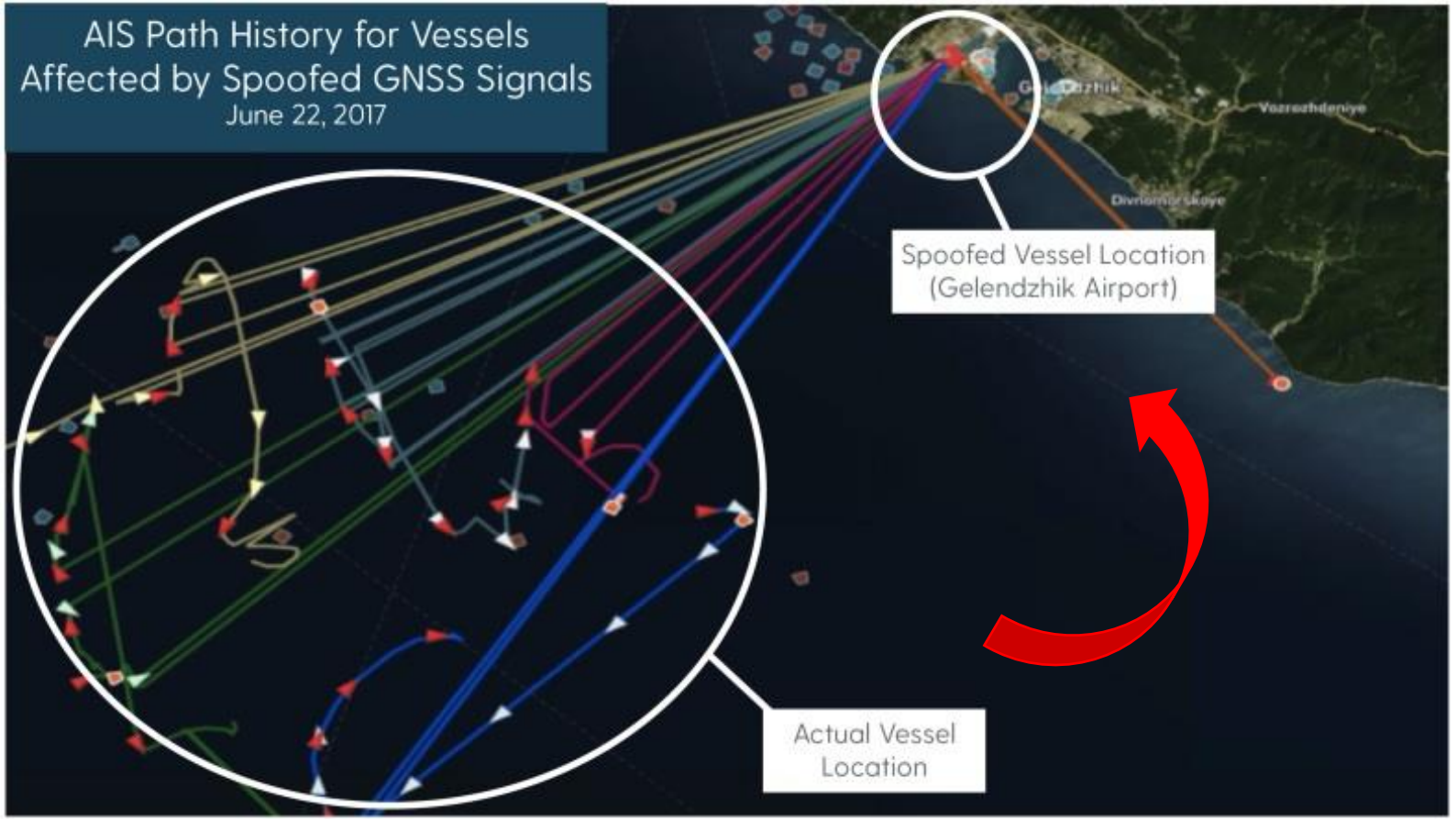
研究背景

- GNSSの利用を妨害する手段にスプーフィングがある
- 攻撃者は偽の位置情報を放送し、被害者は偽の位置/時間情報を得る



参照：https://insidegnss.com/under-attack-receiver-response-to-spoofing-robustness-vs-resilience/

研究背景



ロシア、クリミア半島でのスプーフィング攻撃は、民間商船のGPSナビゲーションを妨害した

AISの位置情報が空港へと改ざんされている

参照：https://c4ads.org/reports/above-us-only-stars/#execsum

研究背景

GNSSに依存するシステムに対し、スプーフィングは脅威となる

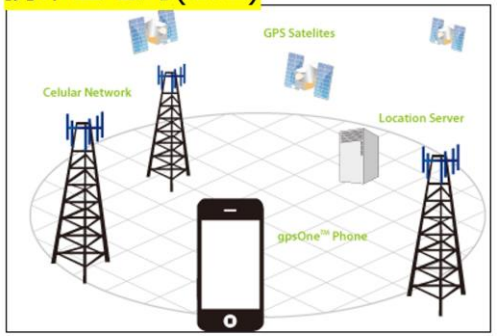
GNSS
(Global Navigation Satellite System)

GPS
QZSS
BDS
GLONASS
GALILEO

スマートグリッド

https://www.furuno.com/jp/gnss/case/smartgrid

携帯基地局(LTE)



https://www.furuno.com/jp/gnss/case/furuno02

UAV

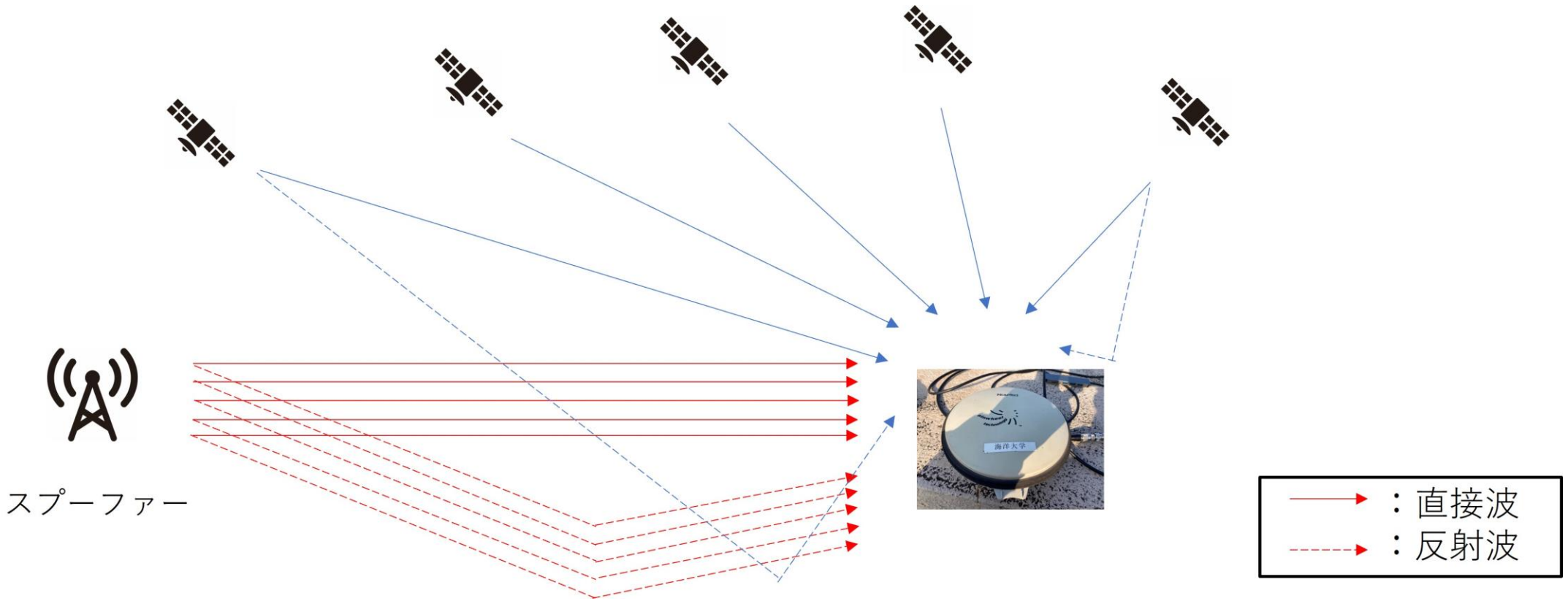
https://en.wikipedia.org/wiki/Phantom_%28unmanned_aerial_vehicle_series%29

自動運転技術

https://www.itmedia.co.jp/news/articles/1910/23/news028.html

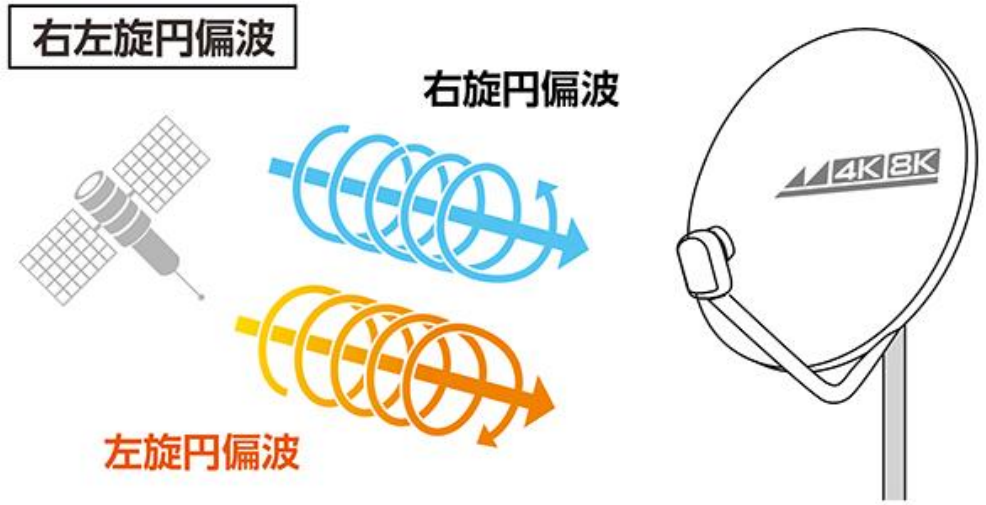
信号到来方向監視

- 実際の衛星からの信号は、様々な距離、角度から放射される一方、スプーファーからの信号は同一方向から放射される



信号到来方向監視

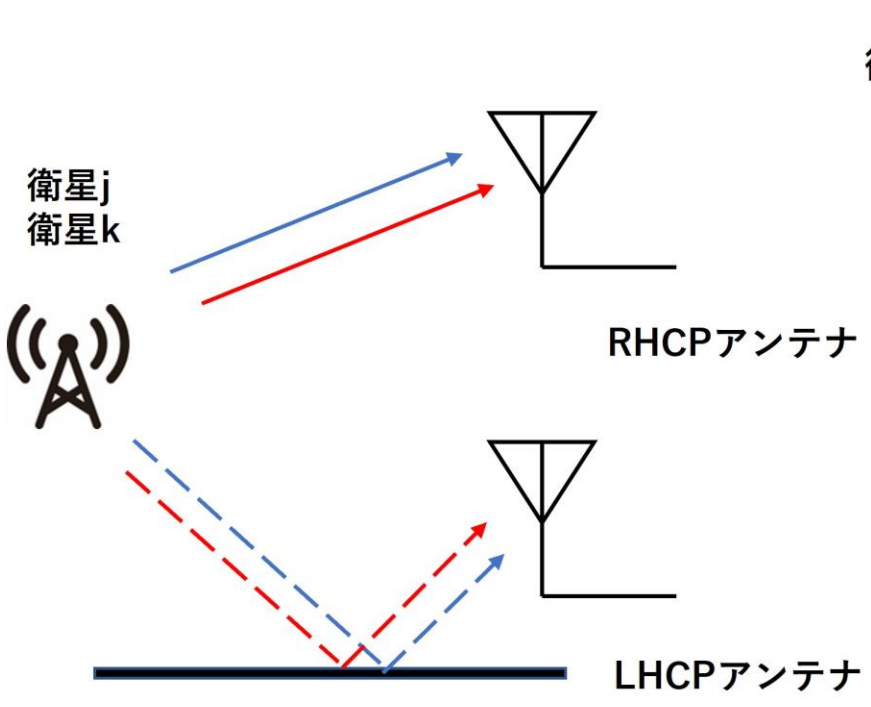
- GNSSでは、RHCP(Right Hand Circular Polarization/右旋円偏波)という偏波方式を採用している。
- 一方、受信機側での電磁界は信号の反射により劣化し、LHCP(Left Hand Circular Polarization/左旋円偏波)の成分が発生する。



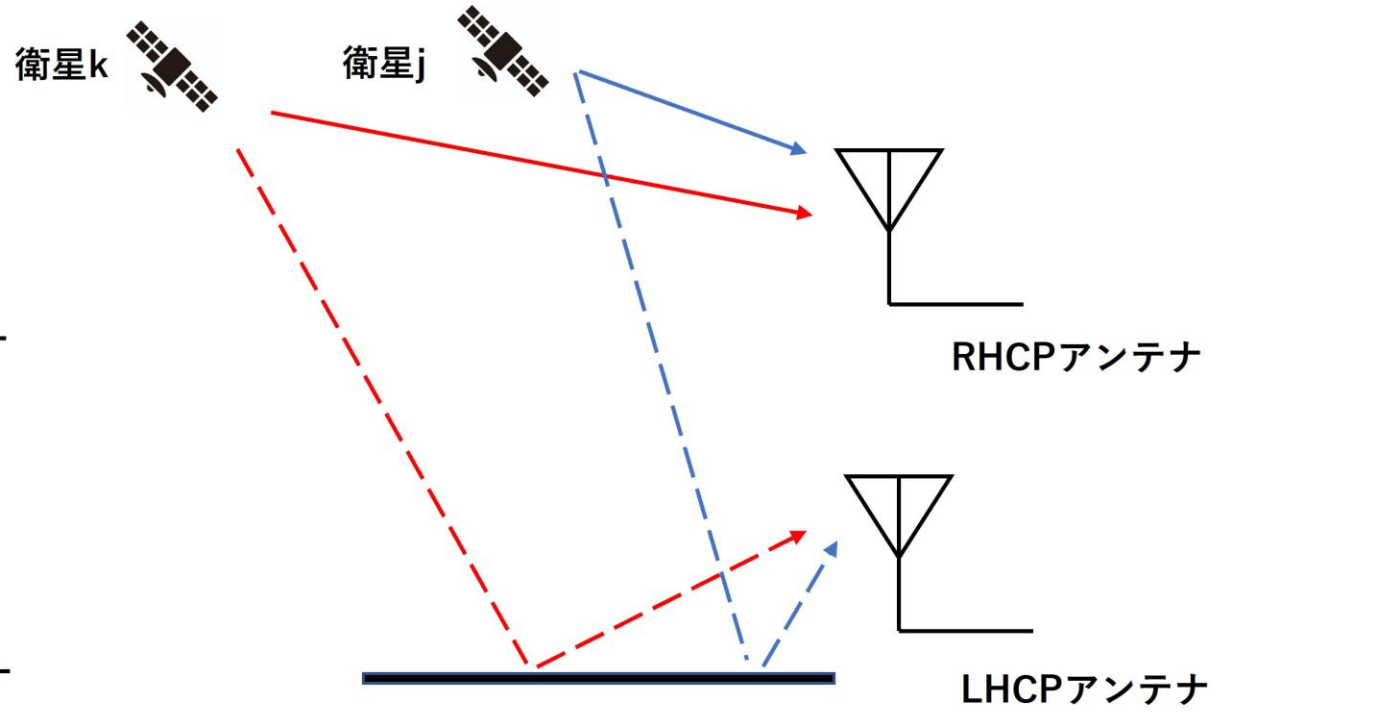
https://www.nichian.net/shop/pages/library-01-basic.aspx

信号到来方向監視

- RHCPアンテナとLHCPアンテナの2つで信号を同時取得する



Spoofingの場合

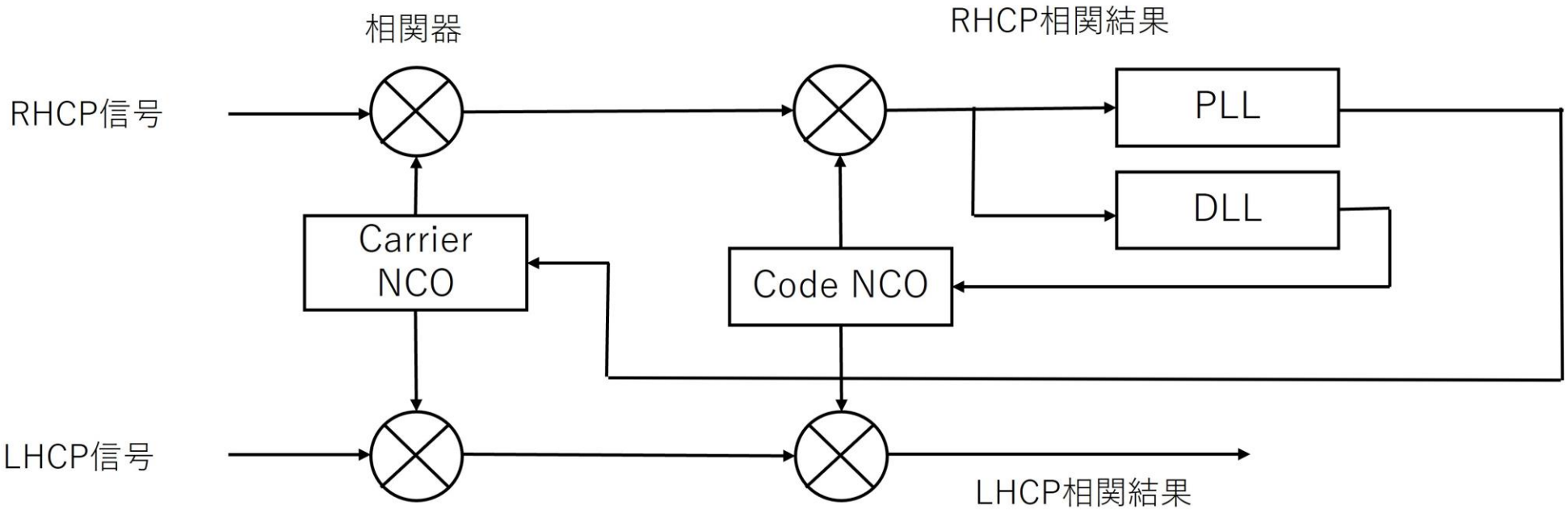


実際の場合

：直接波
：反射波

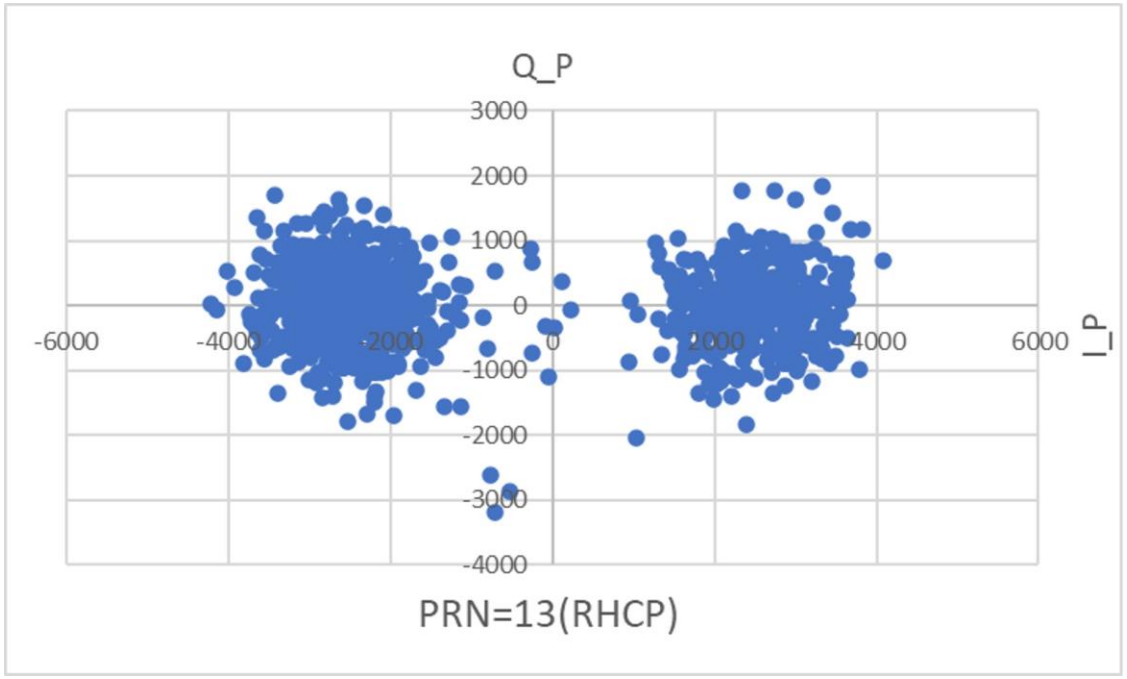
信号到来方向監視

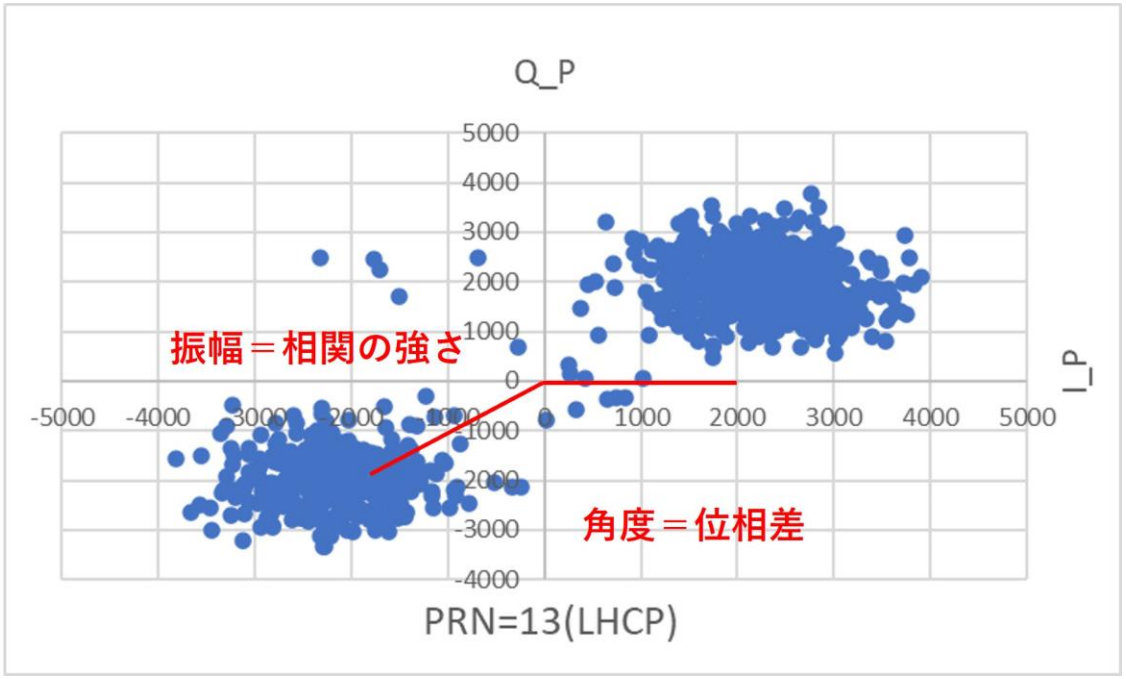
- RHCP信号をソフトウェア受信機で信号捕捉、信号追尾する
- ある衛星の GNSS 信号の 擬似距離コードと相関が取れた場合、相関がとれたポイントの情報を LHCP 信号の相関器に渡して 相関を取ることで同じタイミングにおける反射波の相関値 をＩ相とQ 相で計算する。



信号到来方向監視

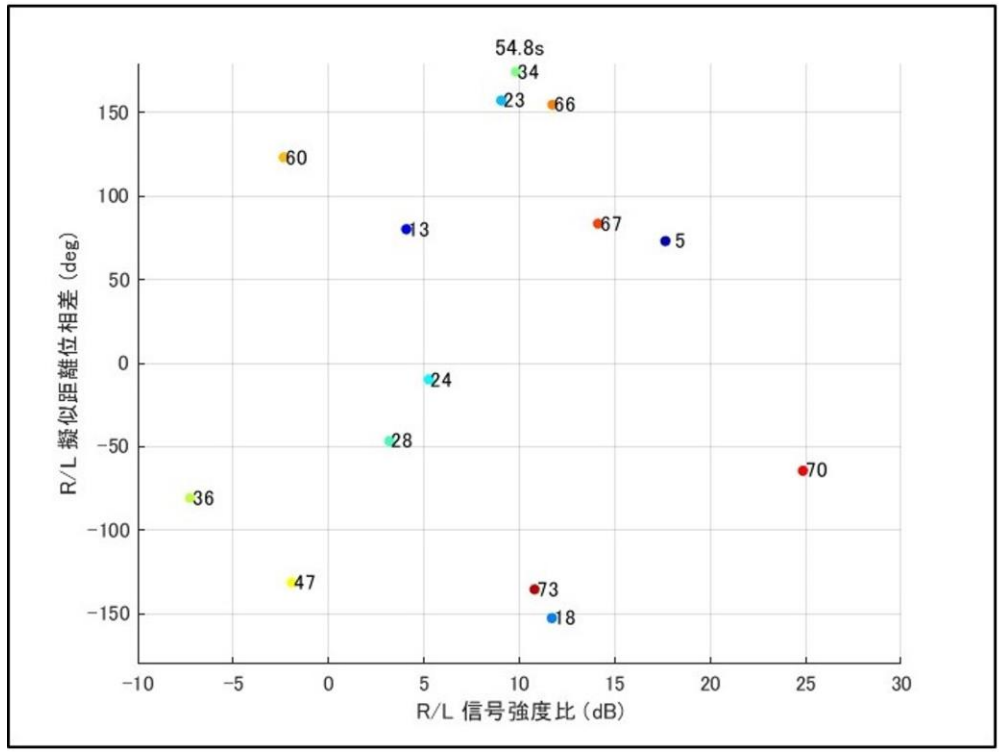
- 信号強度比を相関の強さとして表す
- LHCPはQ相成分が表れ、振幅がRHCPより傾く(位相差)
- この2つをパラメーターで表し、真の衛星とスプーファーで比較

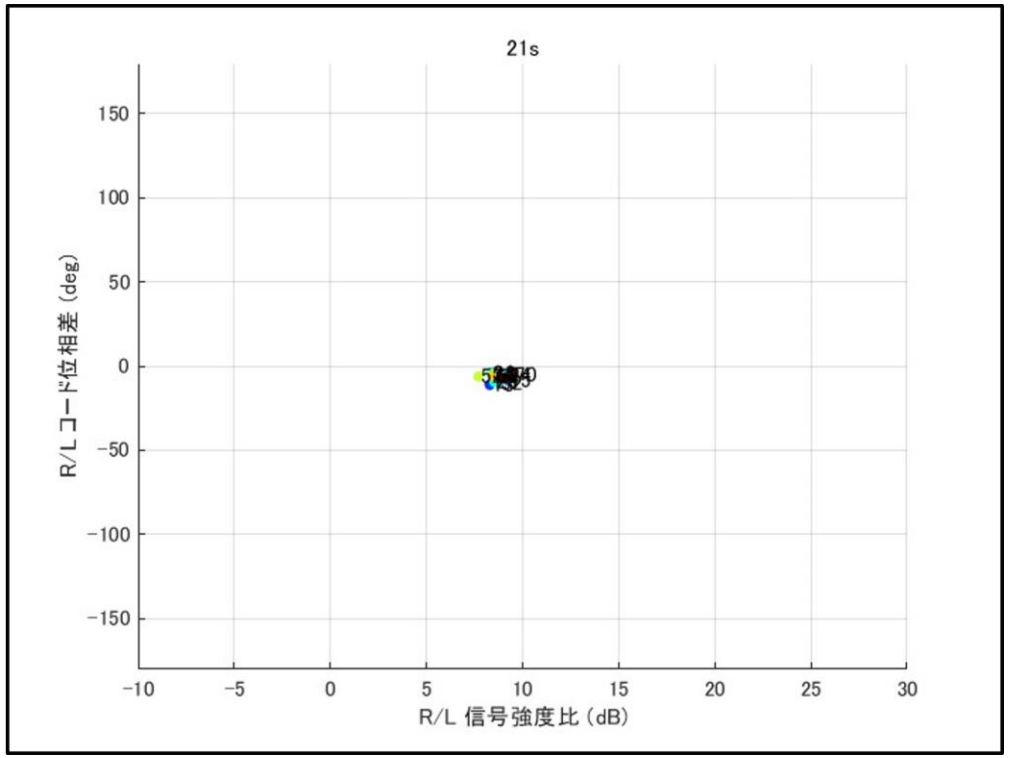




信号到来方向監視

- 左が真の衛星信号、右がスプーファー(屋内)
- パラメーターが類似することで、スプーフィングを検知できる

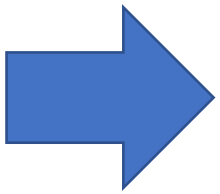




本研究の目的

- 先行研究では、固定した2つのアンテナに対して1方向から
  スプーフィング信号を放射し、高い検知率を得た

- 移動体(船舶など)に対するスプーフィングを想定すると、
  攻撃者と被害者の幾何学的な位置関係は変化していく



信号到来方向が変化する場合のスプーフィング検知

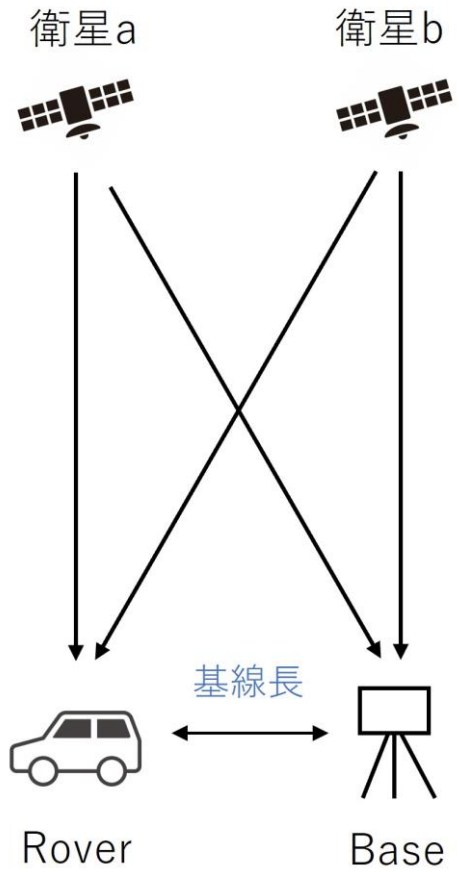
補足(RTKの基礎)

- 搬送波位相観測値について

$$\phi = \lambda\Phi = \rho + c(dt - dT) - I + T + \lambda N + \varepsilon$$

ここで、

ϕ：搬送波位相(m)　　dt：受信機時計誤差(s)
Φ：搬送波位相(cycle)　dT：衛星時計誤差(s)
λ：波長(m)　　I　：電離層遅延量(m)
ρ：衛星-受信機間　　T　：対流圏遅延量(m)
　　幾何学距離(m)　　N　：搬送波位相バイアス(cycle)
c：光速(m/s)　　ε：ノイズ(m)



補足(二重位相差)

- 二重位相差
  →移動局u基準局rにおいて受信した衛星a,bの観測値間で差をとる
- 搬送波位相の二重位相差

$$\phi_{ur}^{ab} = \rho_{ur}^{ab} + c\left(dt_{ur}^{ab} - dT_{ur}^{ab}\right) - I_{ur}^{ab} + T_{ur}^{ab} + \lambda N_{ur}^{ab} + \varepsilon$$

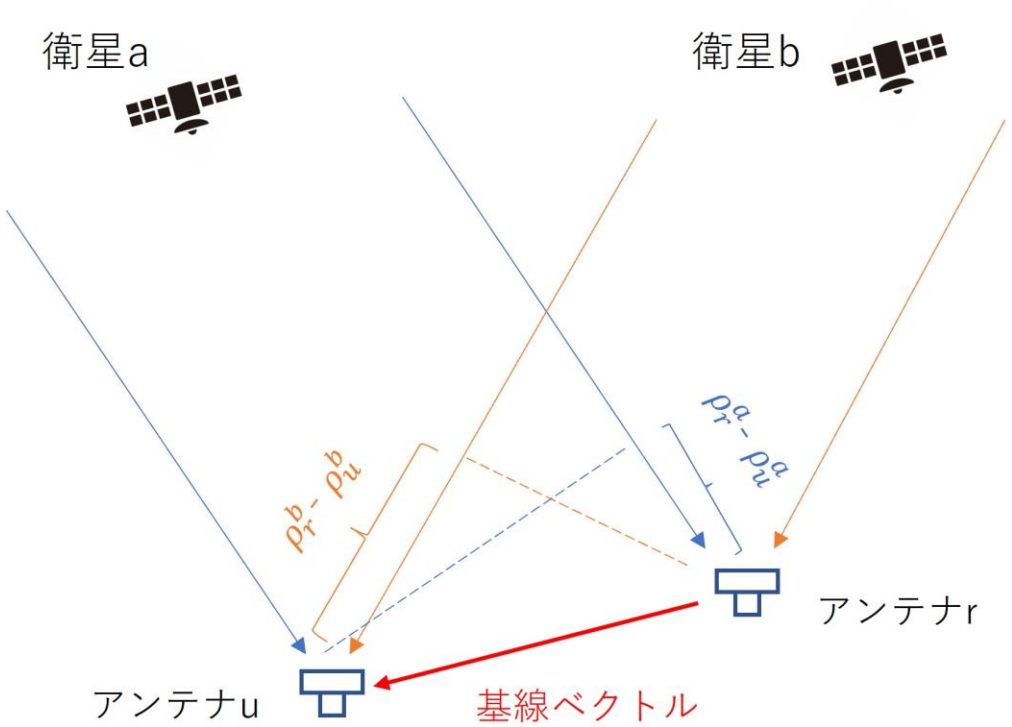
$$dt_{ur}^{ab} = \left(dt_u^a - dt_r^b\right) - \left(dt_r^a - dt_r^b\right) = 0$$
$$dT_{ur}^{ab} = \left(dT_u^a - dT_r^b\right) - \left(dT_r^a - dT_r^b\right) \approx 0$$
$$\mathrm{I}_{ur}^{ab} = \left(\mathrm{I}_u^a - \mathrm{I}_r^b\right) - \left(\mathrm{I}_r^a - dT_r^b\right) \approx 0$$
$$T_{ur}^{ab} = \left(T_u^a - T_r^b\right) - \left(T_r^a - T_r^b\right) \approx 0$$

より

$$\phi_{ur}^{ab} = \rho_{ur}^{ab} + \lambda N_{ur}^{ab} + \varepsilon \quad \text{(短基線モデル)}$$

基線長解析手法

- 真の衛星は衛星信号が様々な方向から到来する。アンテナ間ベクトルの計算を行うと、基線ベクトルは次のように表すことができる。



基線ベクトルは先ほどの二重位相差を用いて、

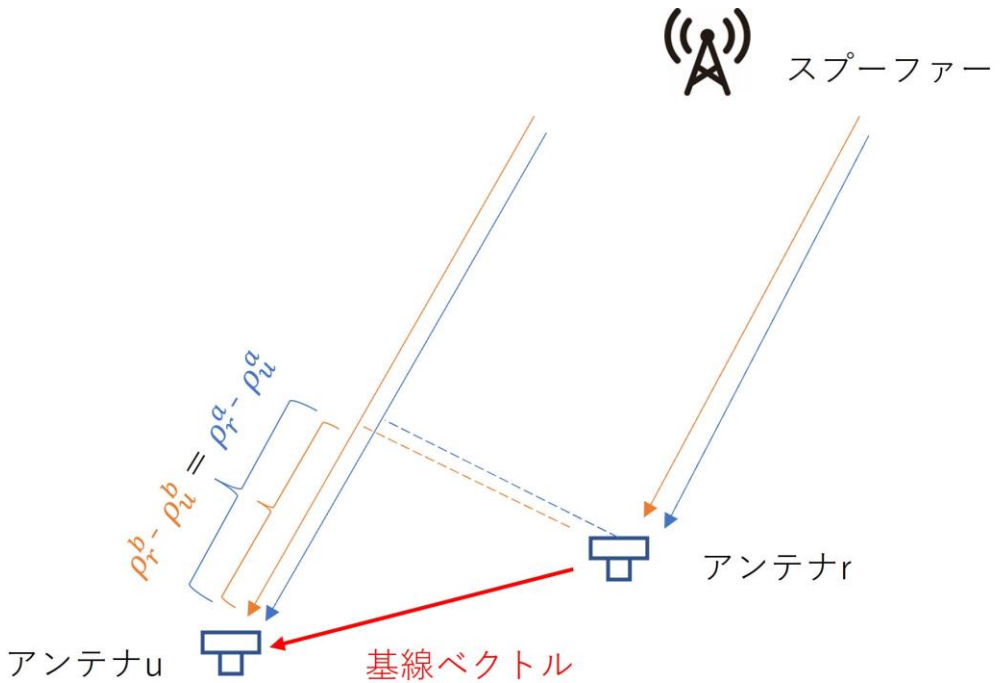
$$\phi_{ur}^{ab} = \phi_{ur}^{b} - \phi_{ur}^{a}$$

$$= \rho_r^b - \rho_u^b - (\rho_r^a - \rho_u^a) + \lambda N_{ur}^{ab} + \varepsilon$$

と表される

基線長解析手法

- スプーフィング信号はすべての衛星信号が同じ方向から到来する。そのため、アンテナ間ベクトルの計算を行うと、基線ベクトルの大きさがゼロとなる。



基線ベクトルは先ほどの二重位相差を用いて、

$$\phi_{ur}^{ab} = \phi_{ur}^{b} - \phi_{ur}^{a}$$

$$= \rho_r^b - \rho_u^b - (\rho_r^a - \rho_u^a) + \lambda N_{ur}^{ab} + \varepsilon$$

スプーフィング中は

$$(\rho_r^b - \rho_u^b - (\rho_r^a - \rho_u^a)) = 0$$

となるためバイアス値のみ残りベクトルの大きさがゼロになる

基線長解析手法

- 基線長解析手法の特徴

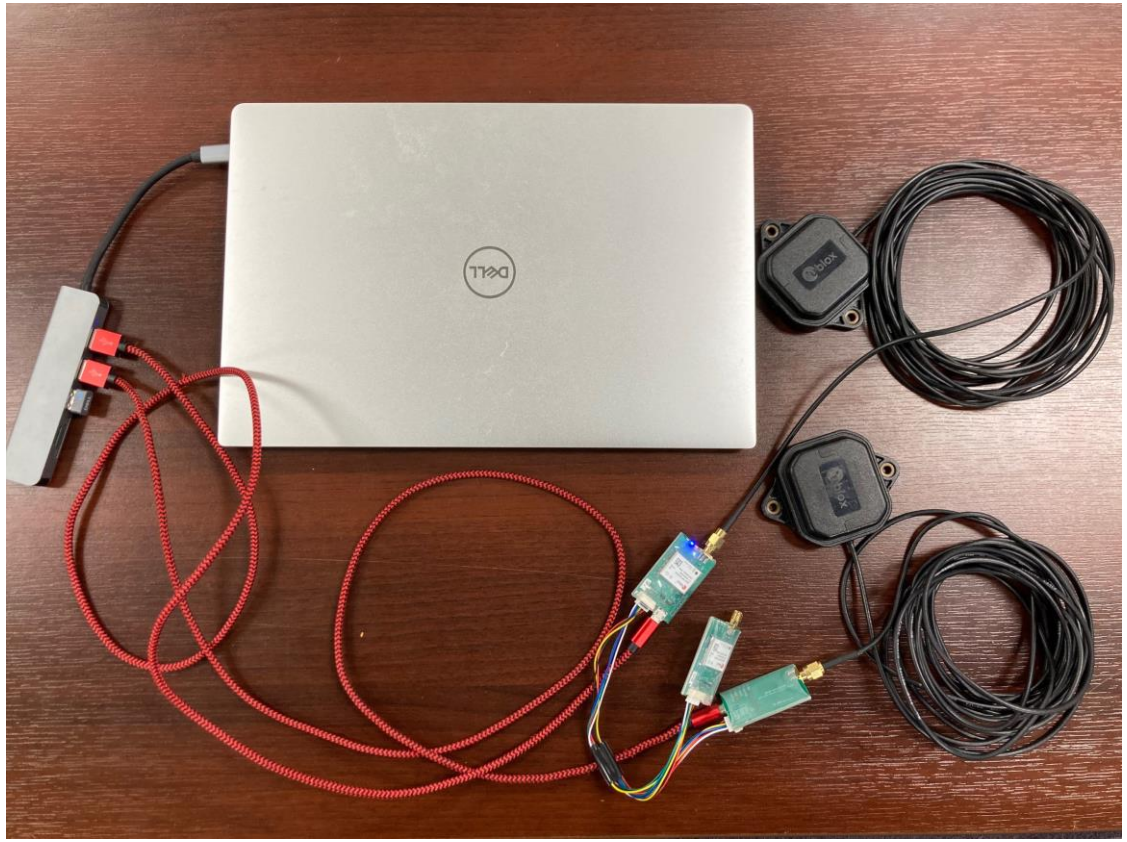
→ 1方向からのスプーフィングに対して検知可能
→ 複数方向からのスプーフィングでは基線ベクトル計算(RTK Fix)ができない

- 複数方向スプーフィング検知の判定

➡ RTK Fixできない場合、スプーフィングが行われていると判断

基線長解析手法

- GNSSコンパスは2アンテナ間の精密なベクトル計算を行う
- 基準側のアンテナから移動局側への方位と相対距離を算出する

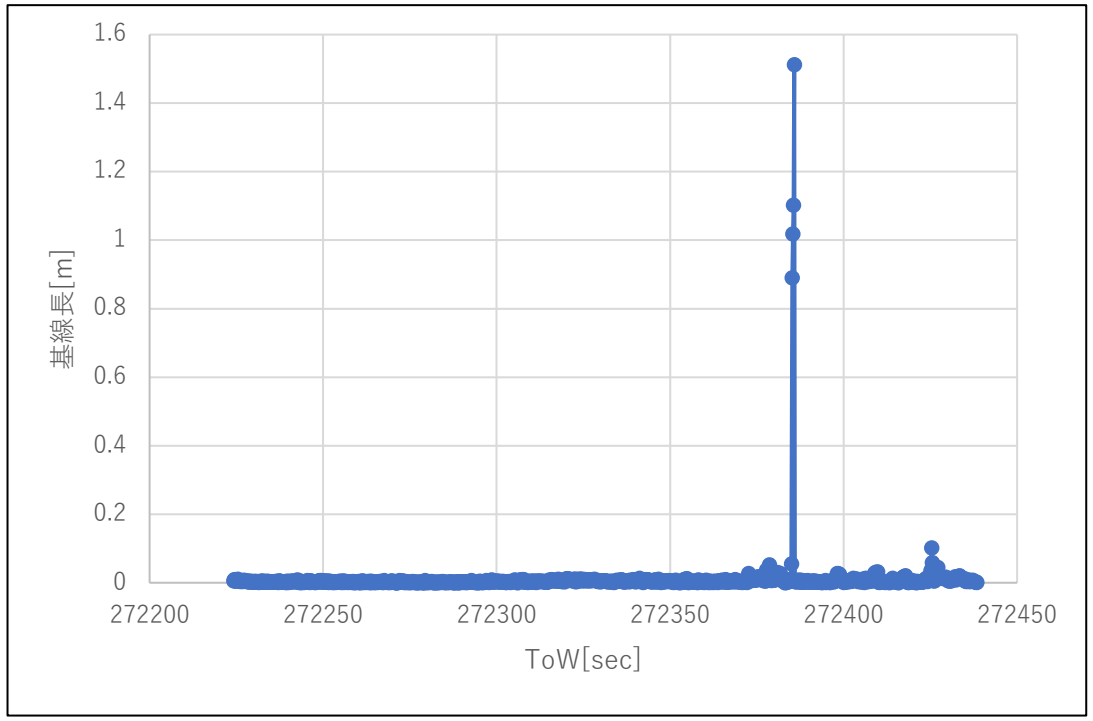


基線長解析手法

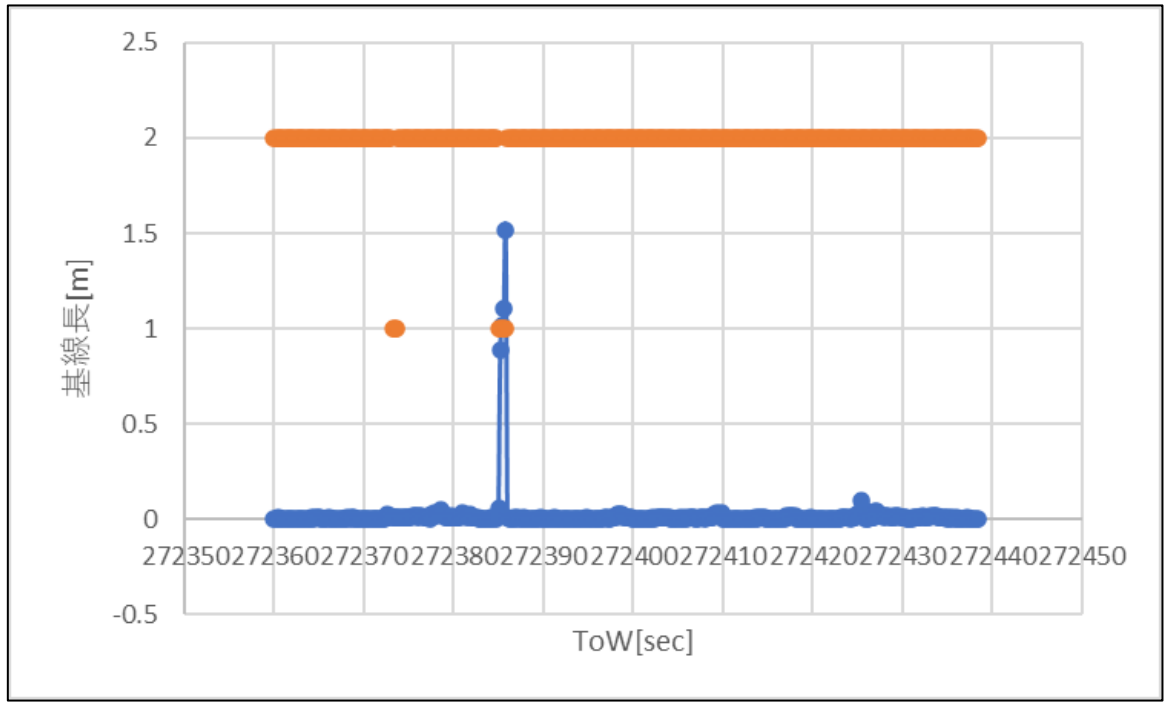
- 2022年10月4日、研究室内で実施、約3分間のデータを取得
- F9Pコンパスを使用して、基線長がゼロになるかを検証した
- 研究室円卓の端から端で約3m離れて再放射をあてた

基線長解析手法

- Ubxファイルを後処理し基線長を求めた(RELPOSNED)
- Float時に値が飛んでいる以外はゼロに収束しているとわかる



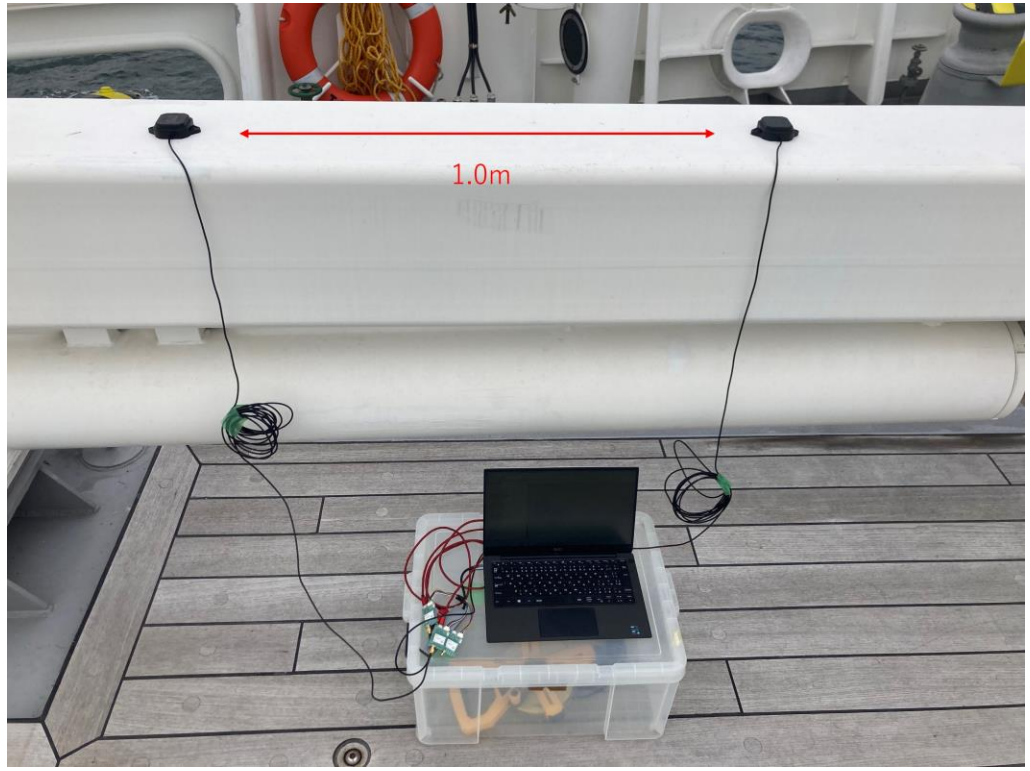
スプーフィング中の基線長



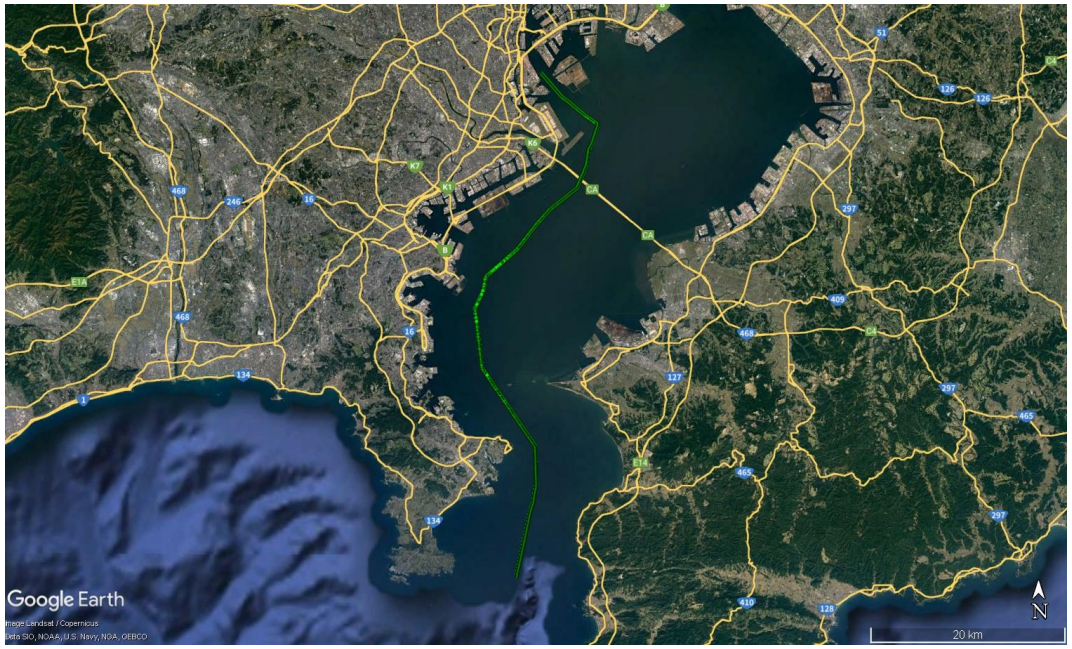
基線長とRTKフラグ

実験1

- 本学所有の汐路丸にて、アベイラビリティと誤検知率の評価を行った。2023年1月19日、実験航海中に約3時間データを取得した。



実験機器構成



航跡

実験1

- GNSSの信号環境が良いほど検知率があがる(アベイラビリティ)
- RTK Fixの判定だが、データ落ちにより基線長がゼロが存在

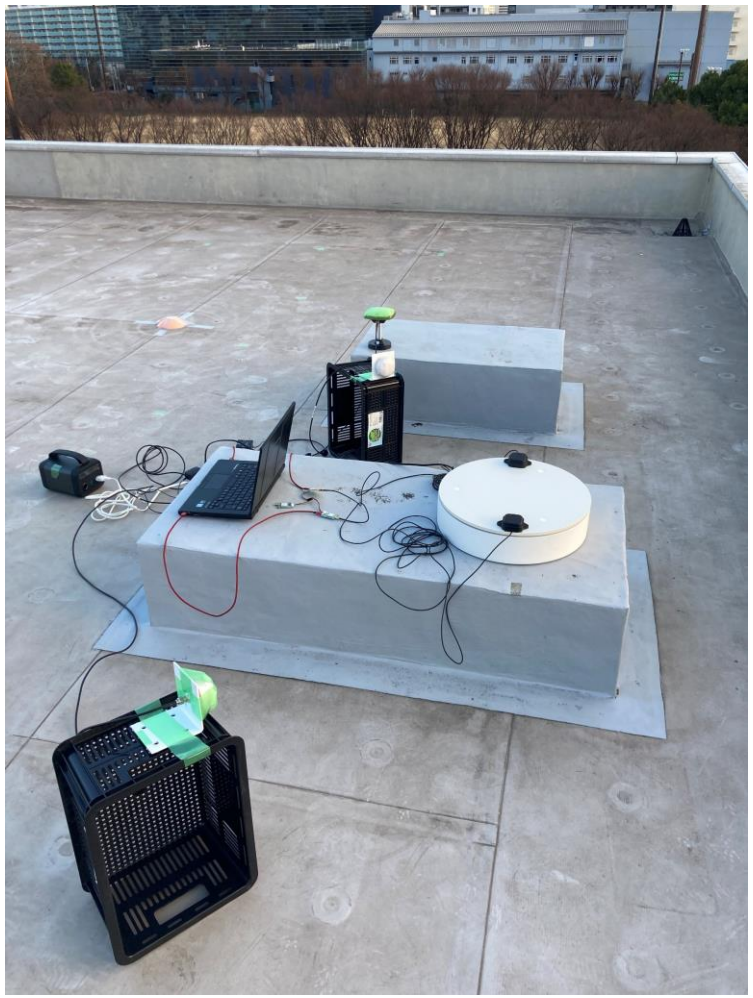
→　計算失敗として扱った

- アベイラビリティは100.00%であった

	Epoch	Percentage		
RTK Fix	49098	100.00%	ミスFix	0.0%
			計算失敗	0.11%
RTK Float	0	0.0%	ミスFix	0.0%
			計算失敗	0.0%
No Result	0	0.0%	-	-
Total	49098	100.00%	-	-

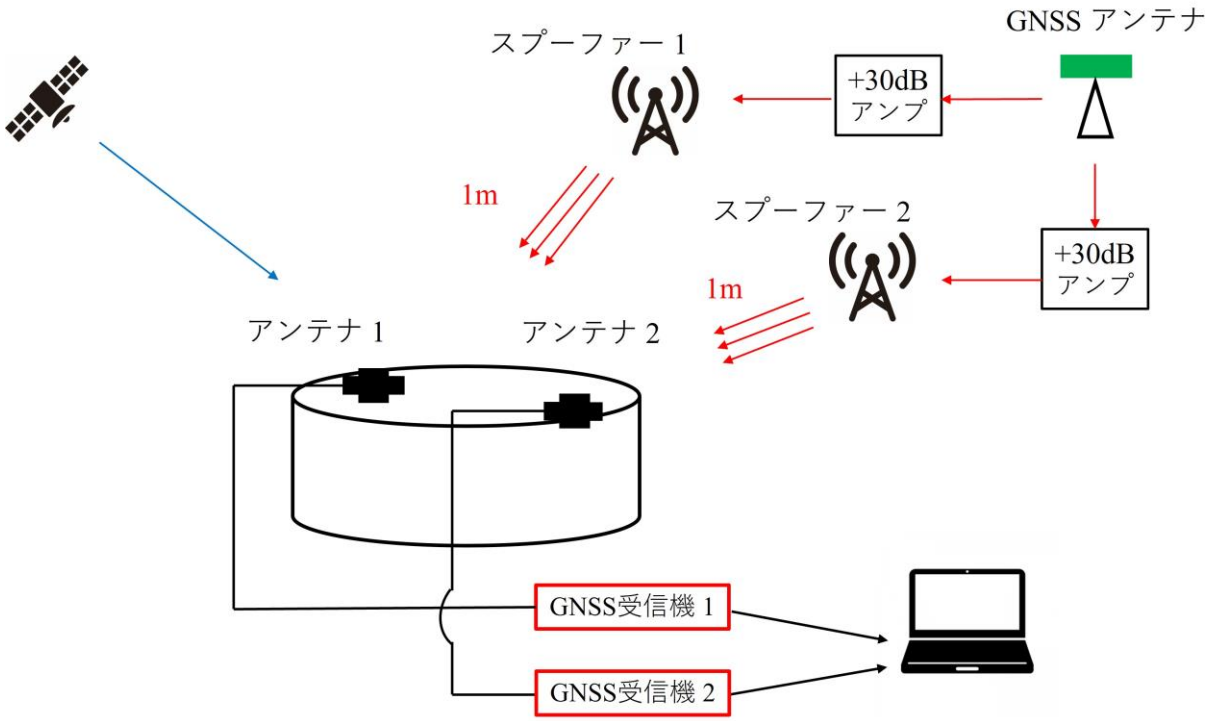
実験2

- 想定環境(船舶上)における検知手法のアベイラビリティを確認した
- 2023年1月2日、東京海洋大学越中島キャンパス第四実験棟屋上にてスプーフィング実験を行った
- 電波法が定める免許不要の出力を遵守し信号を再放射した



実験2

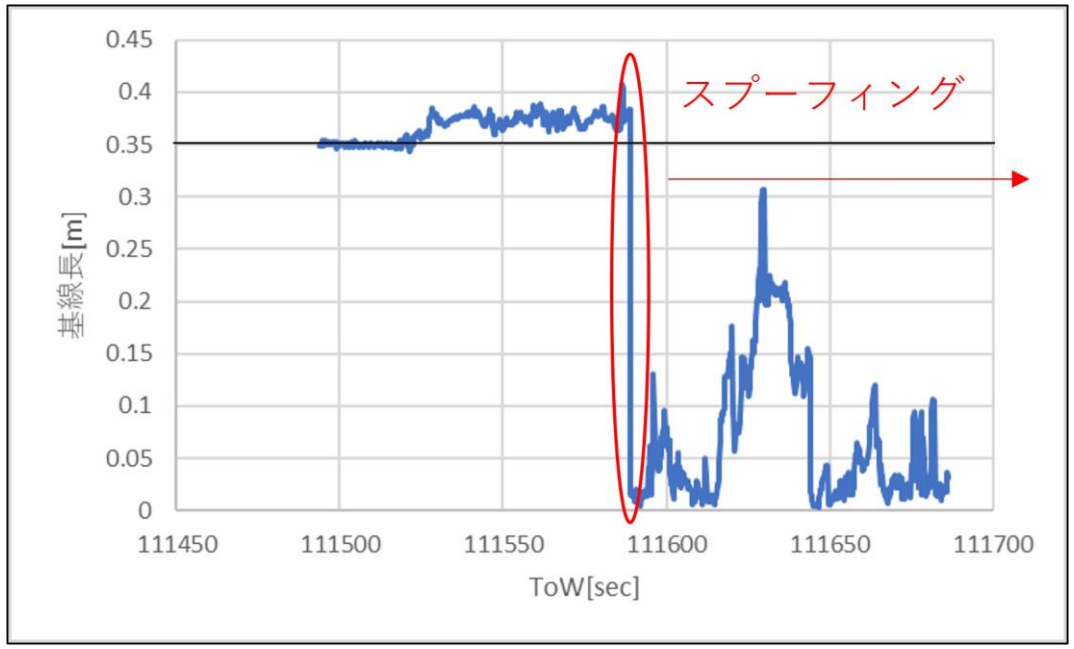
- アンテナ2つを回転テーブルに設置し、約1m離れた1つまたは2つの再放射アンテナから、スプーフィング信号を放射した
- 約3分間データを取得し、約1分後に再放射した



名称	メーカー/型番	説明
アンテナ1	u-blox　ANN-MB-00	L1,L2帯対応
アンテナ2	u-blox　ANN-MB-00	L1,L2帯対応
GNSS受信機1	u-blox　ZED-F9P	マルチGNSS L1,L2,L5帯対応
GNSS受信機2	u-blox　ZED-F9P	マルチGNSS L1,L2,L5帯対応
再放射用受信アンテナ	JAVAD　GrAnt-G3T	L1帯マルチGNSS LNA = 32±2 dB
再放射用送信アンテナ	GPS Networking L1/L2GRRKPA-T Passive GPS Antenna	L1,L2,L5帯 パッシブアンテナ
再放射用アンプ	GPS Networking L1/L2GHNRRKIT-T/5/110 Repeater	1000MHz~1700Mz +30dB

実験2

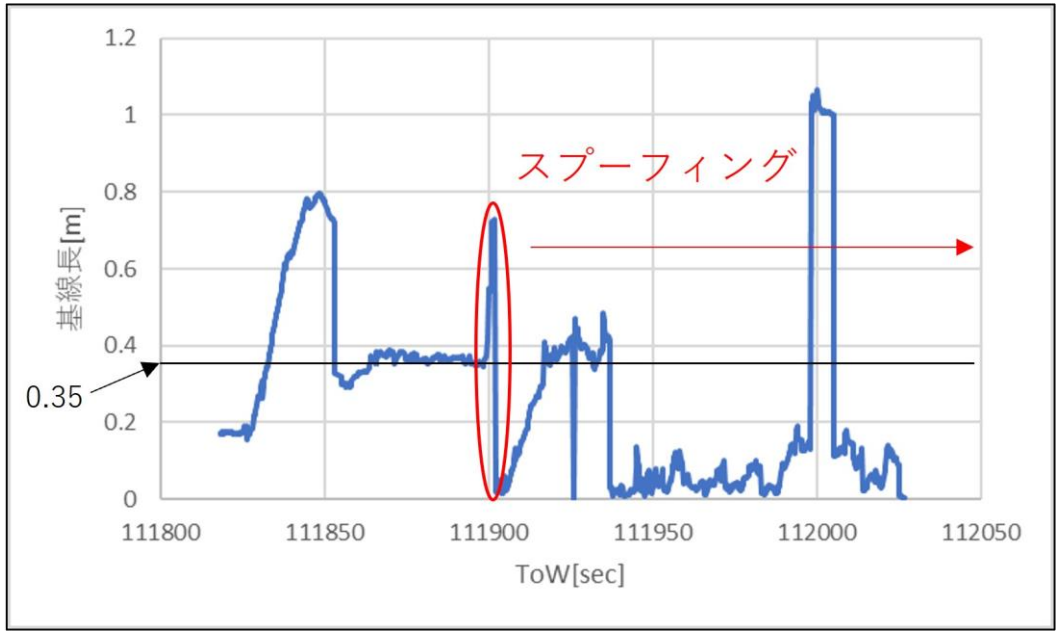
- ① 1方向からスプーフィング信号を放射した場合
- アベイラビリティは 99.17%であった



	Epoch	Percentage		
RTK Fix	483	99.17%	Baseline < 0.05	67.15%
			Baseline ≧ 0.05	32.85%
RTK Float	4	0.83%	Baseline < 0.05	0.00%
			Baseline ≧ 0.05	100.00%
No Result	0	0.00%	-	-
Total	487	100.00%	-	-

実験2

- ② 2方向からスプーフィング信号を放射した場合
- アベイラビリティは 62.74% であった



	Epoch	Percentage		
RTK Fix	389	62.74%	Baseline < 0.05	54.24%
			Baseline ≧ 0.05	45.76%
RTK Float	230	37.10%	Baseline < 0.05	2.17%
			Baseline ≧ 0.05	97.83%
No Result	1	0.16%	-	-
Total	620	100.00%	-	-

結果

- 2方向からスプーフィング信号を放射した結果を示す

- アベイラビリティ(RTK Fix)が低下した→　検知成功
- 基線ベクトル計算の失敗率が上昇した→　追加考察

	1方向	2方向
RTK Fix率	99.17%	62.74%
RTK Float率	0.83%	37.10%
計算成功率	67.15%	54.24%
計算失敗率	0.00%	2.17%

考察

- GNSSコンパス計算について

① 1方向からスプーフィング信号を放射した場合

② 2方向からスプーフィング信号を放射した場合

で比較

Fix解を得て基線長が5cm未満 → 計算成功(通常)

Float解、No Result時に基線長が5cm未満 → 計算失敗

考察

- 2アンテナ間のベクトル計算について

→ RTK Fixができることを前提としている

→ 基線長がゼロとなる検知手法は複数方向からのスプーフィングに適用できない

- ベクトル計算の失敗について

→ 受信機の信号追尾部で出力される搬送波位相が正しく求められない

➡ RTK Fix(搬送波位相)に依存しない代替手法が必要

まとめ

- 2方向スプーフィング実験のRTK Fix率が低下したことより、スプーフィング検知を行った

- GNSSコンパス計算の失敗率を評価した

<今後の課題>

- 様々なスプーフィング攻撃に対応できるように、複数の防御戦略を組み合わせて手法を再構築する

- 移動体(船舶など)に対するスプーフィング実験を行い手法を評価する