GNSSスプーフィングの検知手法の研究

2021/02/09

海運ロジスティクス専攻 1955007 小林海斗

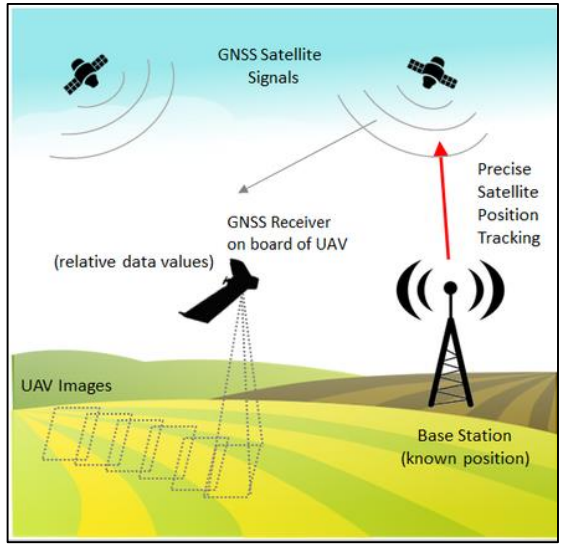
指導教官　久保信明

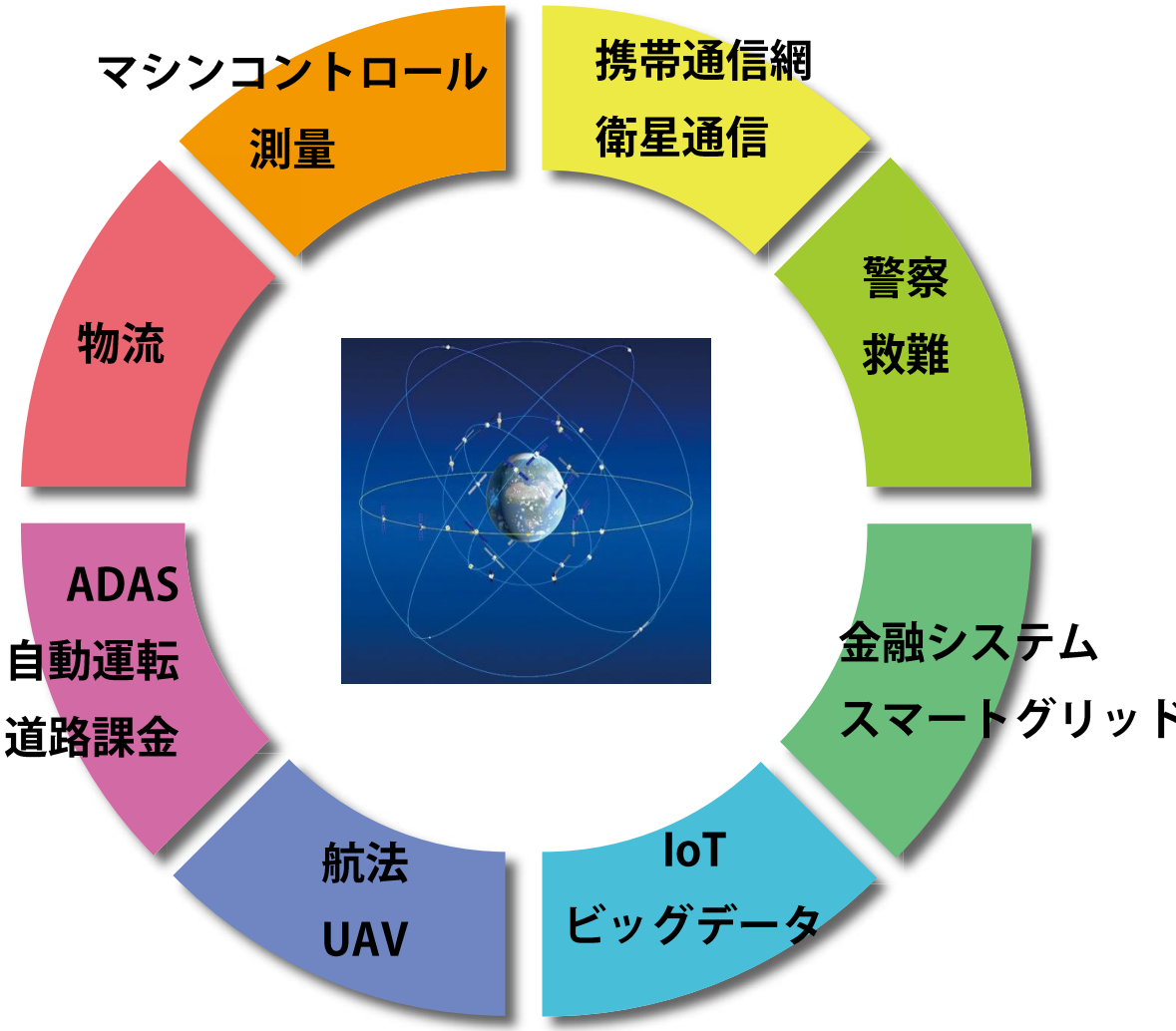
目次

1. 研究背景

◆GNSS（衛星測位）は自身の絶対的な
位置(Position)
速度（Velocity）
時刻(Timing)
を得ることのできるセンサー。

◆現在では様々な産業分野でその利用が進んでいる。





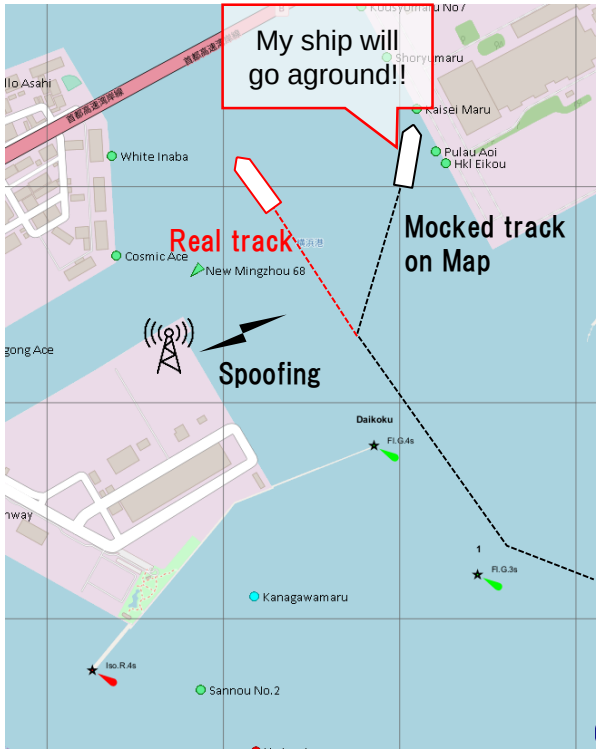
*UAS IMAGERY
https://www.uasimagery.com/

1. 研究背景

◆しかし、GNSSの正常な利用を妨害する手段としてスプーフィングというものがある。
スプーフィング攻撃では偽のGNSS信号を発射し、それを受信したGNSSユーザーは偽の位置情報を得てしまう。

◆偽の位置情報は、それがスプーフィングされたものだとシステムが検知できなかった場合、システムを誤動作させる危険性がある。

◆本研究ではスプーフィングを検知する手法を研究した。



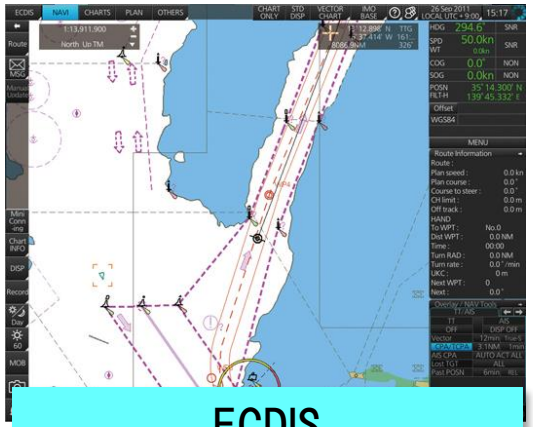
2. 船舶におけるGNSSスプーフィングのリスク

舶用機器は多くがGNSSのPVT情報を利用している。

GNSS

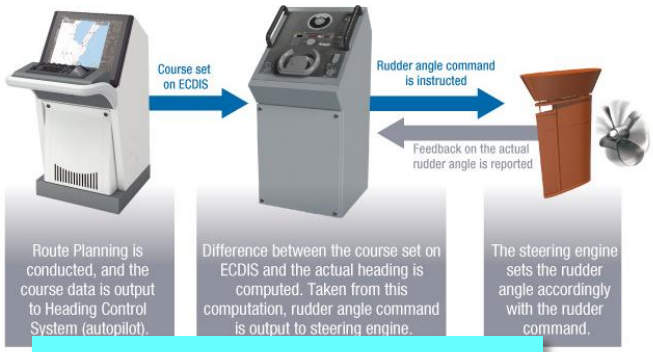
PVT

Speed, Course, Attitude



ECDIS

AIS



Auto Pilot

VDR

Satellite communication

TUMSAT GNSS Lab

*FURUNO HP
https://www.furuno.com/en/merchant/

2. 船舶におけるGNSSスプーフィングのリスク

船舶運航の将来的な目標として

・遠隔操船

・自動離着桟　などがある

↓

これらの実現にはより正確性が担保された自船のPVT情報が必要。

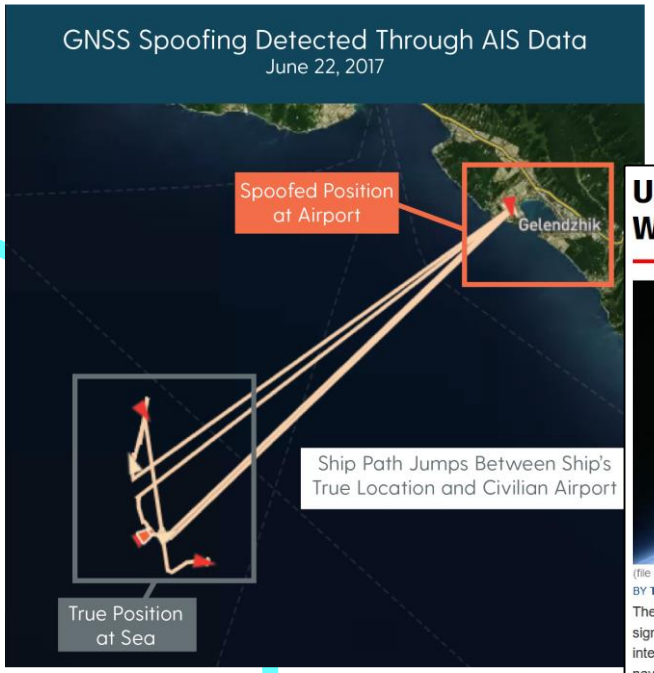
2. 船舶におけるGNSSスプーフィングのリスク

しかし、実際にはスプーフィング機材の低価格化や軍事的なスプーフィングの利用の広まりにより、海上におけるGNSSの信頼度の低下が発生している。

$10,000

$200

低コストスプーフィングリスクの増加



*C4ADS report
https://www.c4reports.org/aboveusonlystars

スプーフィング被害の実例

*The Maritime Executive
https://maritime-executive.com/article/u-s-issues-renewed-mariner-warning-on-gps-interference

座礁、衝突事故のリスク

TUMSAT GNSS Lab

3. 研究ターゲット

船舶において最適なスプーフィング検知手法はなにか…

- **バックアップセンサーの利用**
  大洋航行中は周囲に目標物がなく、船の動揺の問題もありセンサーフュージョンには多くの課題がある。
  (IMU、ドップラーソナー+ジャイロコンパス、レーダーSLAM、etc…)

- **衛星信号側での対策**
  Galileo, QZSSなどで検討は進んでいるが、国家規模のため整備に時間がかかる。(暗号化、電子署名、etc…)

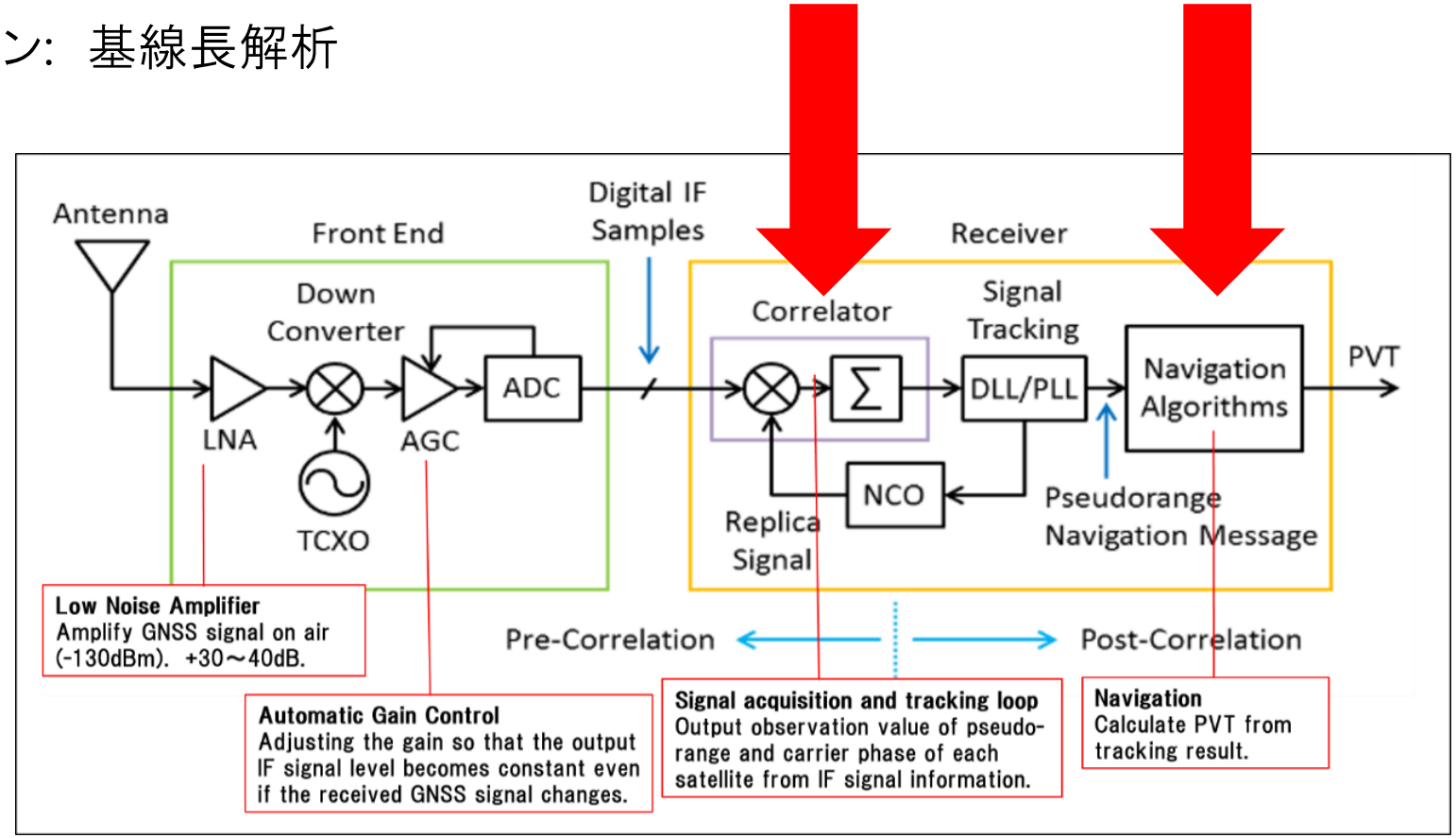
- **受信機側での対策**
  従来の舶用GNSSの機能付加のため、大規模なシステム設計が不要である。
  船舶においてスプーフィングを受ける環境はモデル化が容易なため難易度が低い。

本研究では船舶環境に適用可能な受信機側でのスプーフィング検知手法を2つ提案した。

3. 研究ターゲット

GNSS受信機の2箇所のポイントでスプーフィング検知を試みた。

1. プレコリレーション: マルチパスモニタリング
2. ポストコリレーション: 基線長解析



GNSS受信機内部の処理フロー

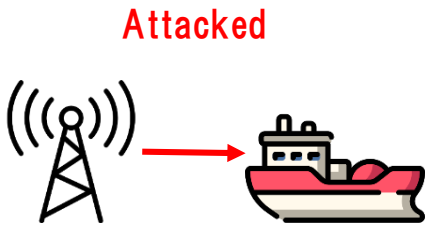
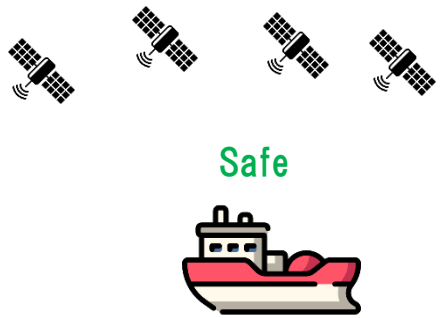
3. 研究ターゲット

提案手法を

・スプーフィングの見逃しがないか

・スプーフィングの誤検出がないか

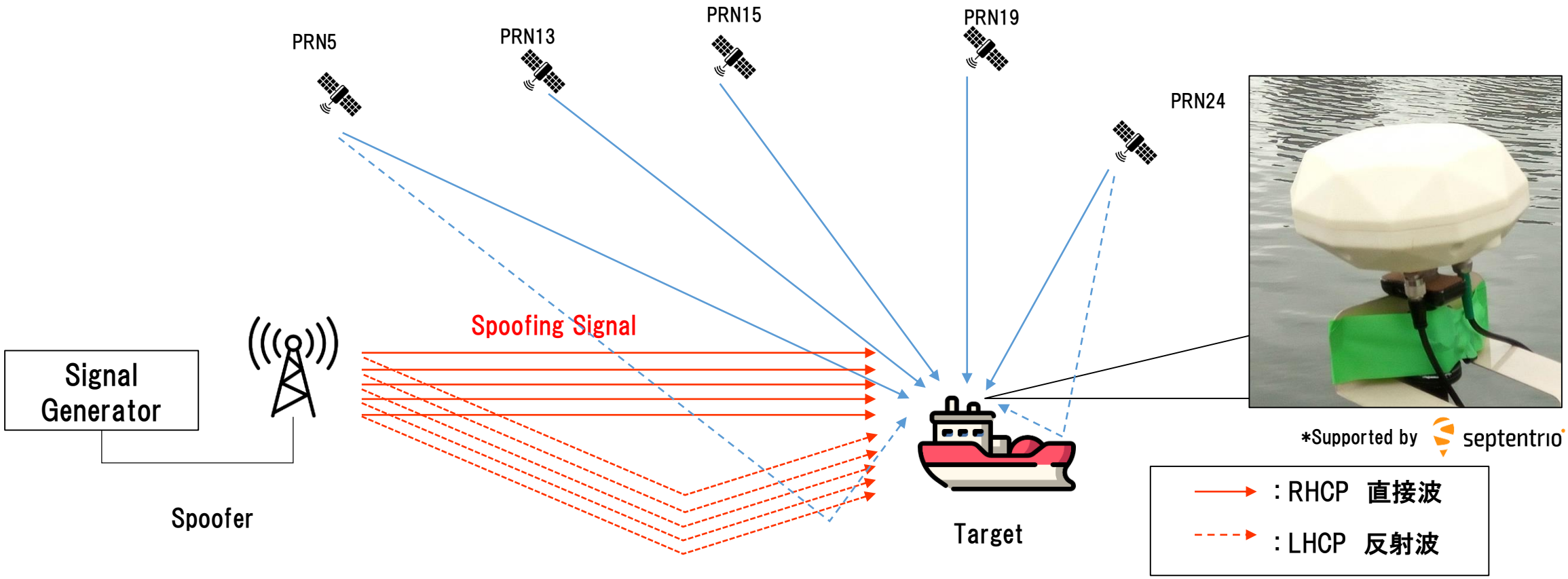
に焦点を当てて評価実験を実施した。

見逃し	
実際の環境	スプーフィング検知システム
	Safe
誤検出	
実際の環境	スプーフィング検知システム
	Spoofing detected

4. マルチパスモニタリングによるスプーフィング検知手法

衛星からの信号とスプーファーからの信号で反射波の経路の特徴に違いがあることに注目した。

スプーフィング信号では全ての衛星の信号が類似した経路で反射波を生成するため、マルチパスのパラメーターに類似性が生じる。



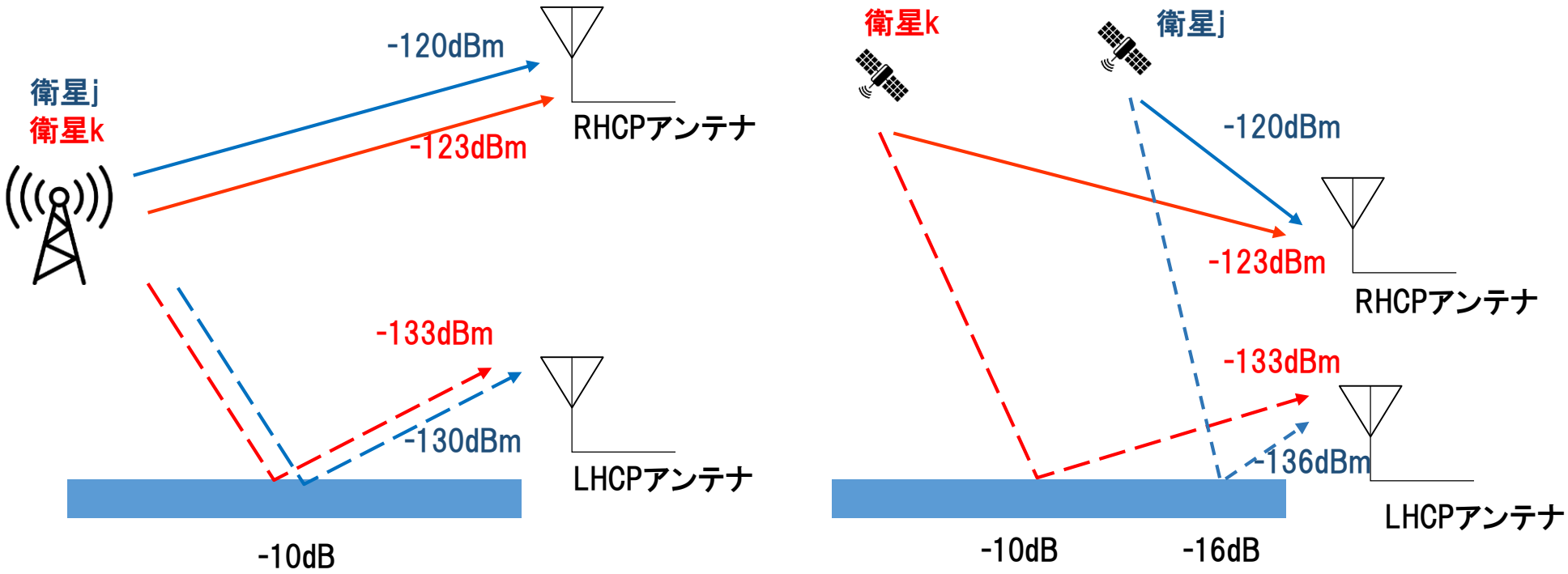
4. マルチパスモニタリングによるスプーフィング検知手法

マルチパスの特徴を2つのパラメーターで表現した。

$$\frac{R}{L}\text{信号強度比}\,[dB] = 20 \cdot log10 \cdot \left|\frac{Ip(R) + i \cdot Qp(R)}{Ip(L) + i \cdot Qp(L)}\right|$$

$$\frac{R}{L}\text{擬似距離位相差}[degree] = \arctan(a, b) \qquad \left(\frac{\mathrm{Ip(R)+i\cdot Qp(R)}}{\mathrm{Ip(L)+i\cdot Qp(L)}} = a + i \cdot b\right)$$

Ip：I相相関値
Qp：Q相相関値
(R)：直接波の信号
(L)：反射波の信号

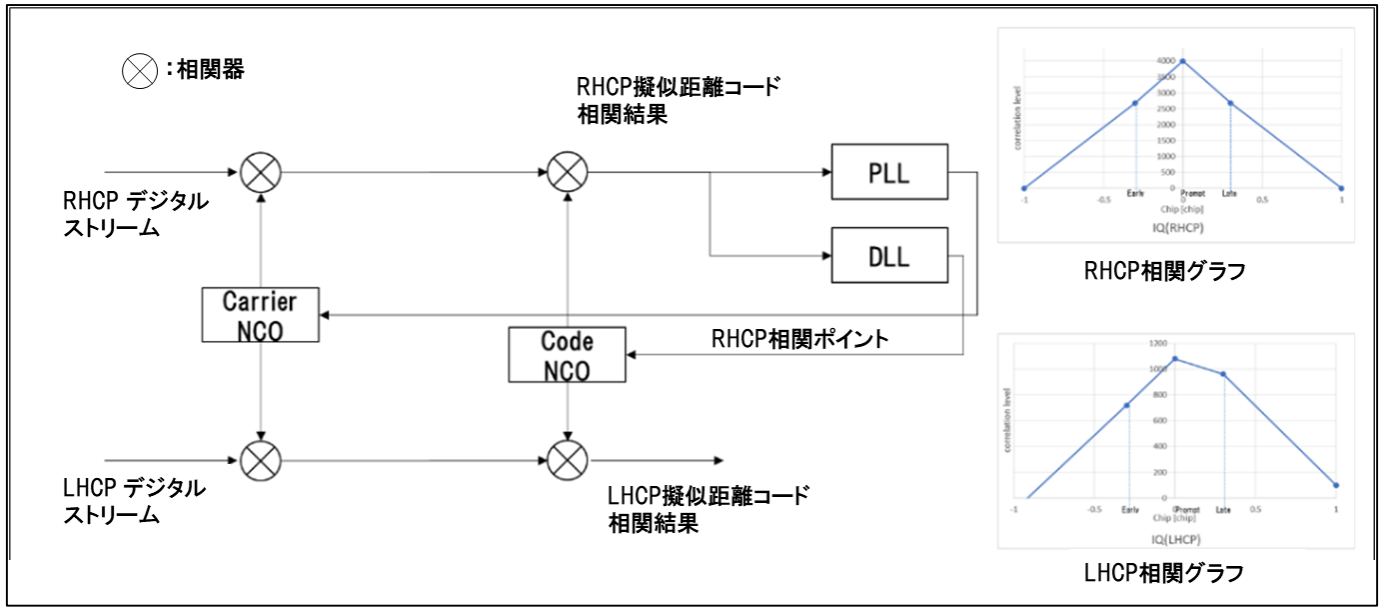


二偏波アンテナで受信された直接波(R) と反射波(L)は2chのソフトウェア受信機によって処理され、エポックごとに各衛星で2つのパラメーターが推定される。

$$\frac{R}{L}\text{信号強度比}\,[dB] = 20 \cdot log10 \cdot \left|\frac{Ip(R) + i \cdot Qp(R)}{Ip(L) + i \cdot Qp(L)}\right|$$

$$\frac{R}{L}\text{擬似距離位相差}[degree] = \arctan(a, b) \qquad \left(\frac{\mathrm{Ip(R)+i\cdot Qp(R)}}{\mathrm{Ip(L)+i\cdot Qp(L)}} = a + i \cdot b\right)$$

Ip : I相相関値
Qp : Q相相関値
(R) : 直接波の信号
(L) :反射波の信号



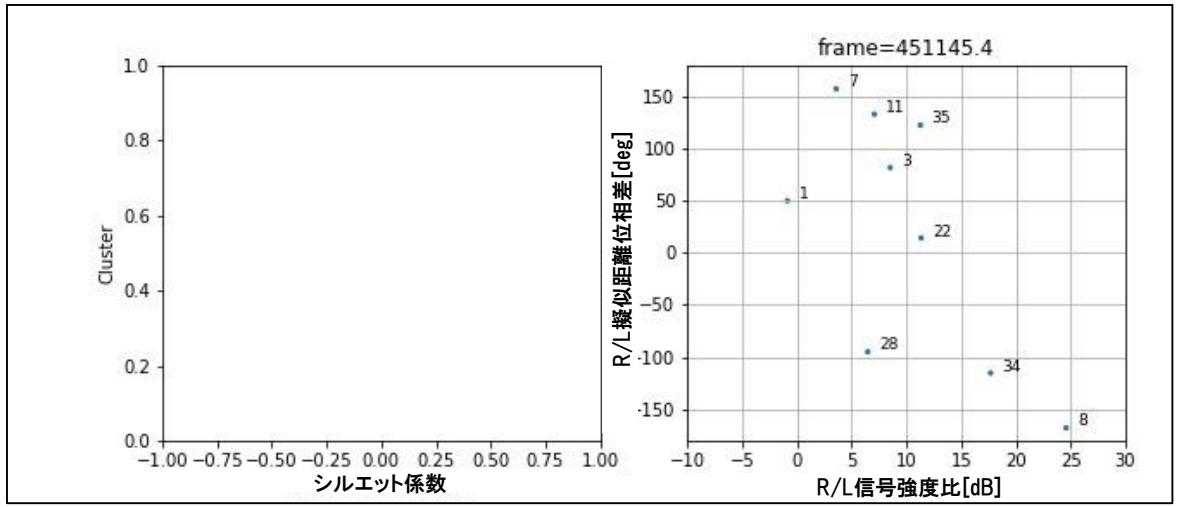
ソフトウェア受信機での2ch処理フロー

4. マルチパスモニタリングによるスプーフィング検知手法

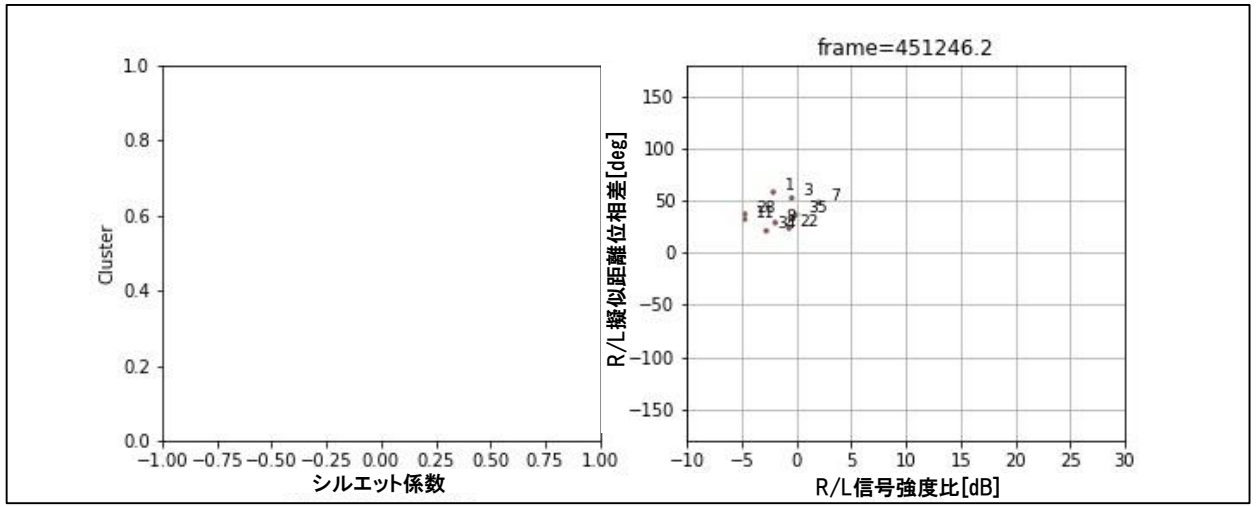
マルチパスの2パラメーターを水平プロットすると図のようになる。

各衛星のパラメーターが類似するとクラスターを形成するため、これをDBSCANクラスタリングアルゴリズムで検出した。

DBSCAN(Density-Based Spatial Clustering of Applications with Noise):　点群の密度とノイズを考慮してクラスタリングする教師なし機械学習。



全て本物の衛星信号
（クラスターなし）



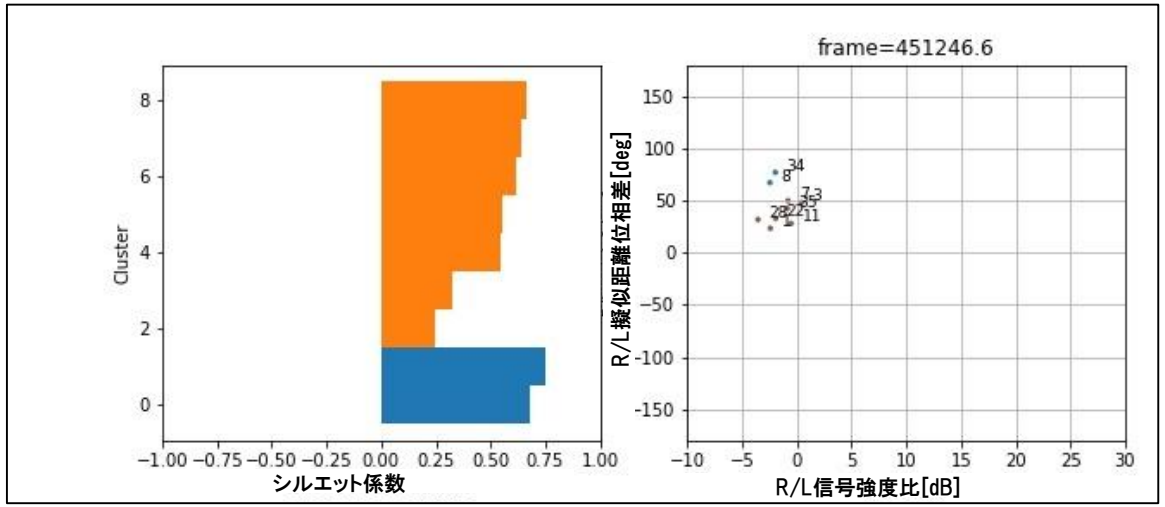
全ての衛星がスプーフィング信号
（1つのクラスター）

4. マルチパスモニタリングによるスプーフィング検知手法

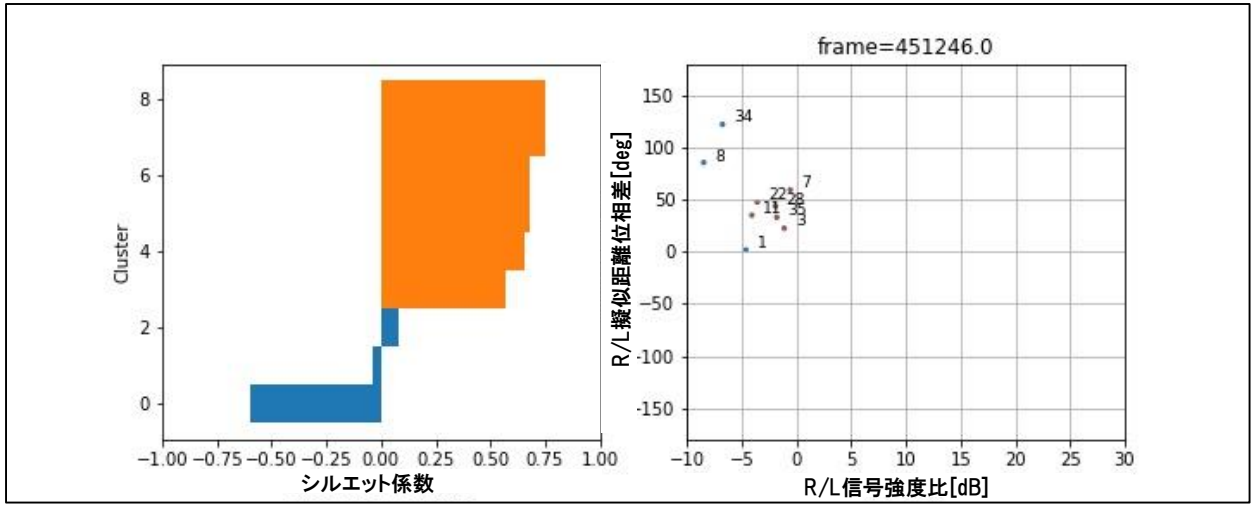
マルチパスの2パラメーターを水平プロットすると図のようになる。

各衛星のパラメーターが類似するとクラスターを形成するため、これをDBSCANクラスタリングアルゴリズムで検出した。

DBSCAN(Density-Based Spatial Clustering of Applications with Noise):点群の密度とノイズを考慮してクラスタリングする教師なし機械学習。



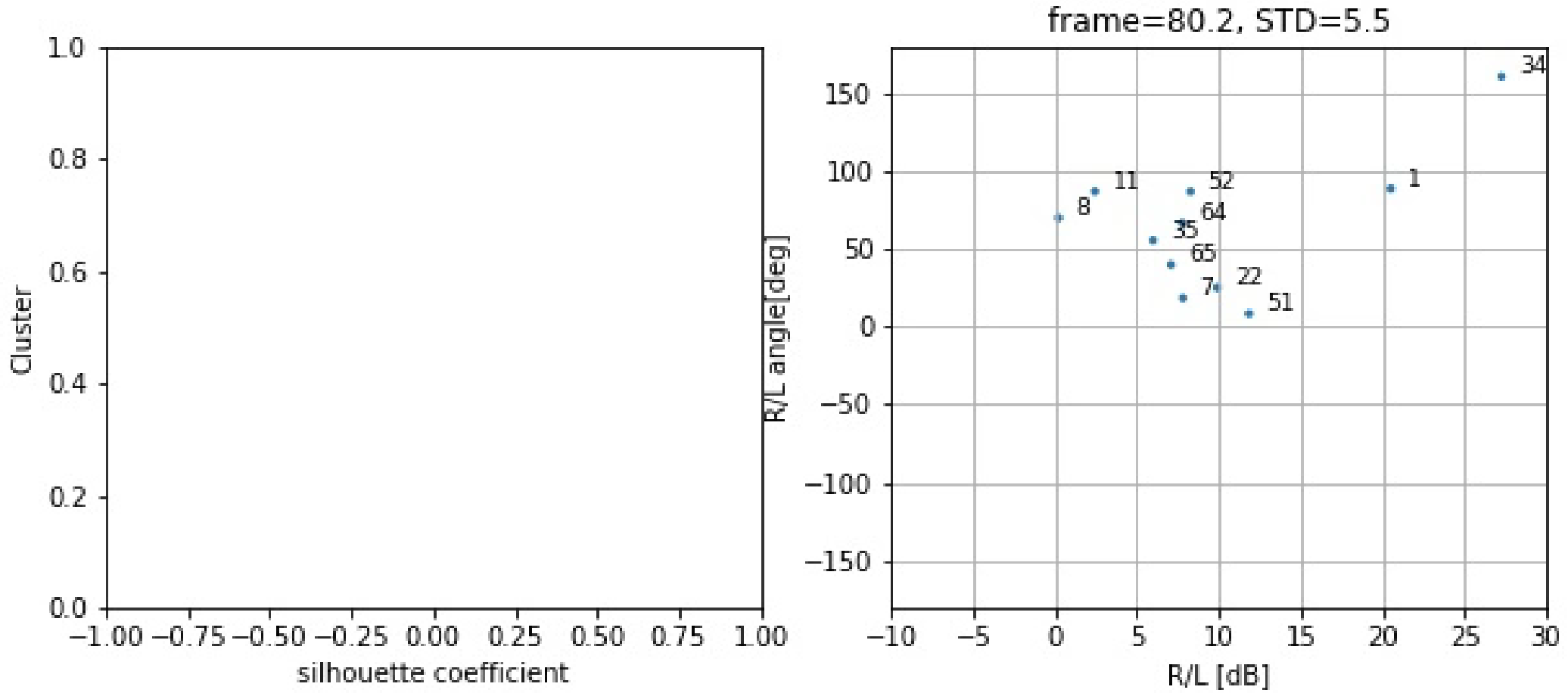
全ての衛星がスプーフィング信号
（2つのクラスター）



6つの衛星がスプーフィング信号
（1つの密なクラスターと1つの粗なクラスター）

4. マルチパスモニタリングによるスプーフィング検知手法

【動画】 スプーフィングなし→スプーフィング中 (frame=96~)



5. 評価実験1

マルチパスモニタリング
船上実験

マルチパスモニタリングによるスプーフィング検知手法の誤検出率を船上実験で確認した。

2020/10/23 汐路丸にて実験航海中、浦賀水道航路で20分間のデータを取得。

アンテナはコンパスデッキの右舷側に設置。

汐路丸上のアンテナ設置位置

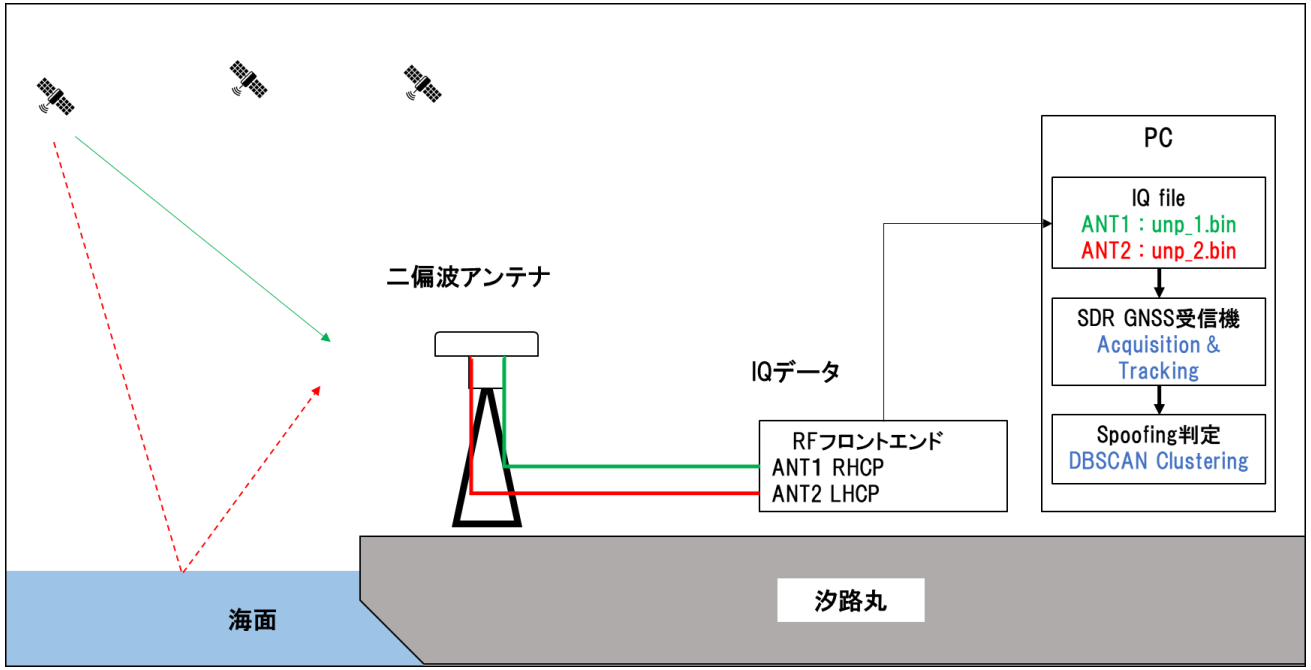
データ取得中の航跡

5. 評価実験1

マルチパスモニタリング
船上実験

2chのRFフロントエンドを用いてL1帯1周波のGNSS信号を取得。

GNSSソフトウェア受信機でGPS, QZSS, Galileo衛星の信号を追尾、クラスタリングを行った。



実験構成図

実験機材

名称	メーカー	詳細
アンテナ	FANTASTIC project	RHCPとLHCPの2偏波アンテナ L1,L2,L5 band LNA 38dB
RFフロントエンド	IP Solution	2ch入力 中心周波数=1575.42MHz IF=4.092MHz サンプリングレート=16.368MHz 2bitのIQ値によるサンプリング
SDR GNS受信機	–	2ch入力 GPS L1C/A, QZSS L1C/A, Galileo E1b
リファレンス受信機	Septentrio	AsteRx-m2 GPS+QZSS+Galileo+GLONASS+BDS

5. 評価実験1

マルチパスモニタリング
船上実験

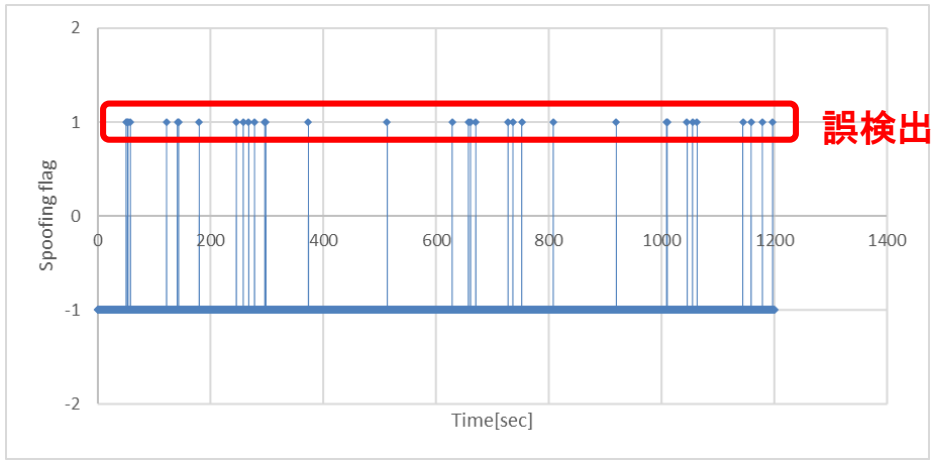
クラスタリングの結果、スプーフィングが誤検出されたのは34エポック(0.6%)であった。

偶発的かつ散発的な誤検出を除去するためにクラスタリング結果の範囲付き時間積分値であるSpoofing levelを設定した。

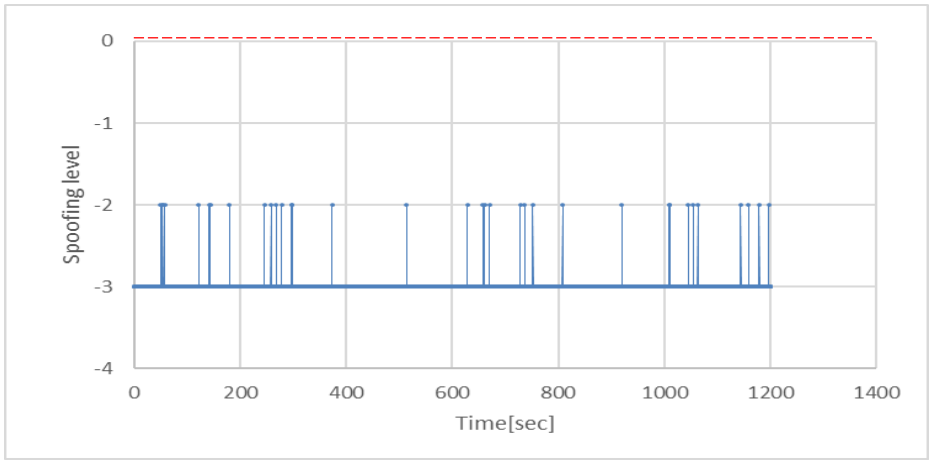
	Epoch	Percentage
Total epoch	6000	100.0%
Spoofing flag=true	34	0.6%
Spoofing flag=false	5965	99.4%

$$Spoofing\ level = \sum_{i=0}^{t} Spf_i \quad (-3 \leq Spoofing\ level \leq 3)$$

Spoofing level≧0のときアラートを発生させる。



Spoofing flagの時系列グラフ



Spoofing levelの時系列グラフ

5. 評価実験1

マルチパスモニタリング
スプーフィング実験

マルチパスモニタリングによるスプーフィング検知手法の見逃し率をスプーフィング実験で確認した。

2020/05/22 東京海洋大学越中島キャンパスポンドにてスプーフィングを行いそのデータを取得。

スプーフィングは3mの距離から再放射を利用して再現した。

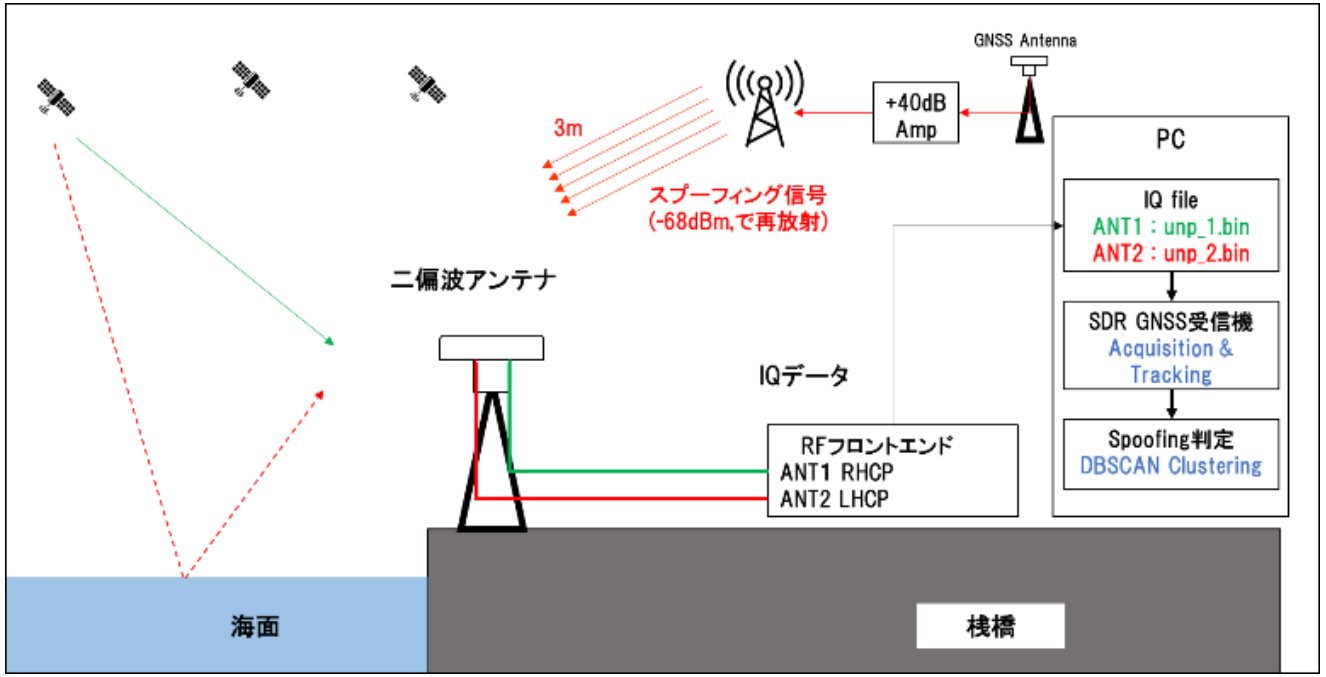
実験環境

5. 評価実験1

マルチパスモニタリング
スプーフィング実験

2chのRFフロントエンドを用いてL1帯1周波のGNSS信号を取得。

GNSSソフトウェア受信機でGPS, QZSS, Galileo衛星の信号を追尾、クラスタリングを行った。



実験構成図

実験機材

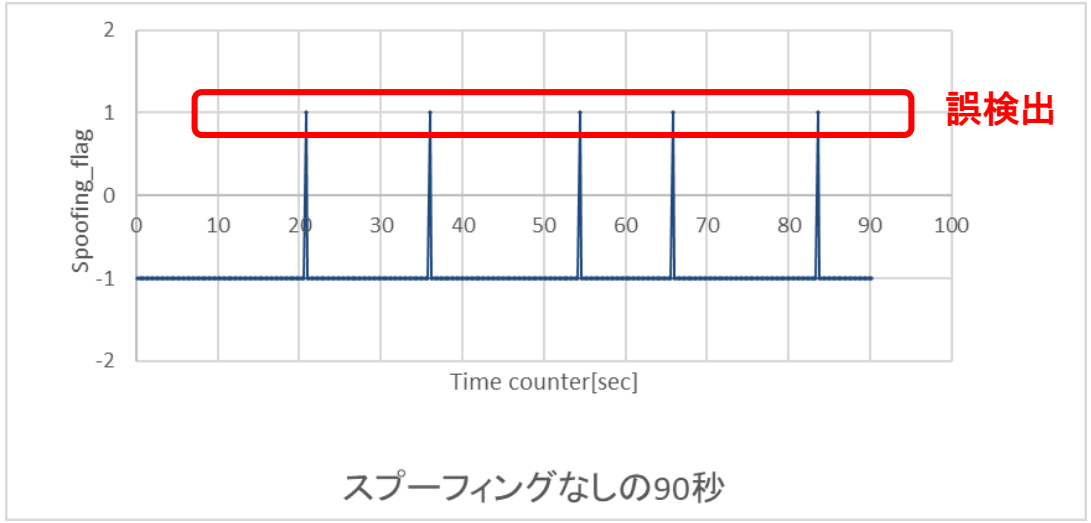
名称	メーカー/型番	説明
二偏波アンテナ	FANTASTICプロジェクト	L1,L2,L5帯 LNA=38dB
RFフロントエンド	IP Solution	2ch入力 中心周波数=1575.42MHz IF=4.092MHz サンプリングレート =16.368MHz 2bit IQサンプリング
SDR GNSS受信機	研究室	2ch並列処理 GPS L1C/A Galileo E1b QZSS L1C/A
リファレンス用受信機	ublox M8T	L1帯マルチGNSS GPS+BDS+Galileo+QZSS
再放射用受信アンテナ	Tallysman TW4722	L1帯マルチGNSS LNA=23dB
再放射用送信アンテナ	GPS source GNSS-3P	L1,L2,L5帯 パッシブアンテナ
再放射用アンプ	ミニサーキットZX60-2534MA	500MHz-2500MHz +39.4dB at 1.5GHz

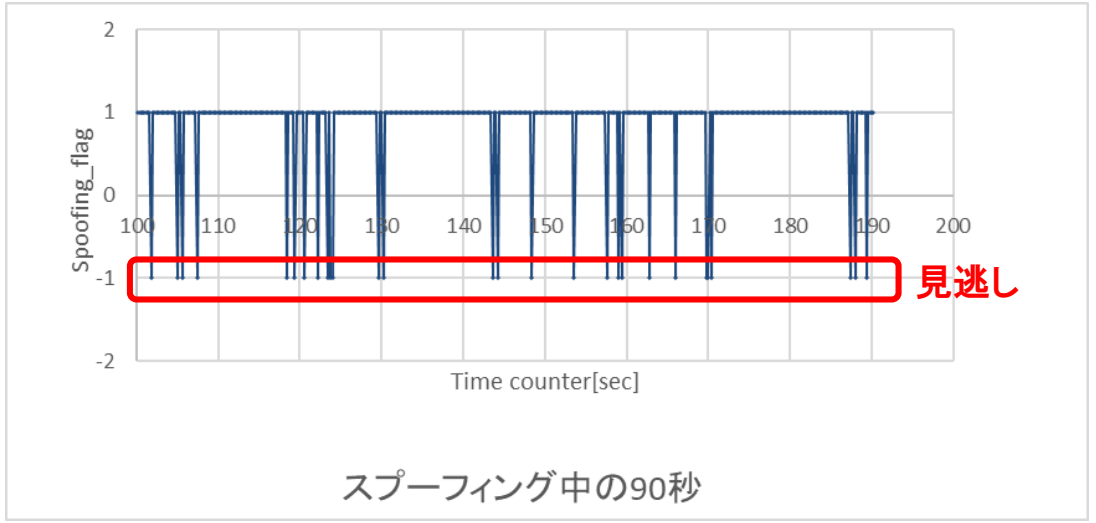
5. 評価実験1

マルチパスモニタリング
スプーフィング実験

クラスタリングの結果、スプーフィングが誤検出されたのは0.7%と船上実験とほぼ同じ水準であった。スプーフィング中の見逃し率は6.2%であった。

	スプーフィングなし		スプーフィング中	
Total epoch	450	100.0%	450	100.0%
Spoofing flag=true	5	0.7%	422	93.8%
Spoofing flag=false	445	98.9%	28	6.2%





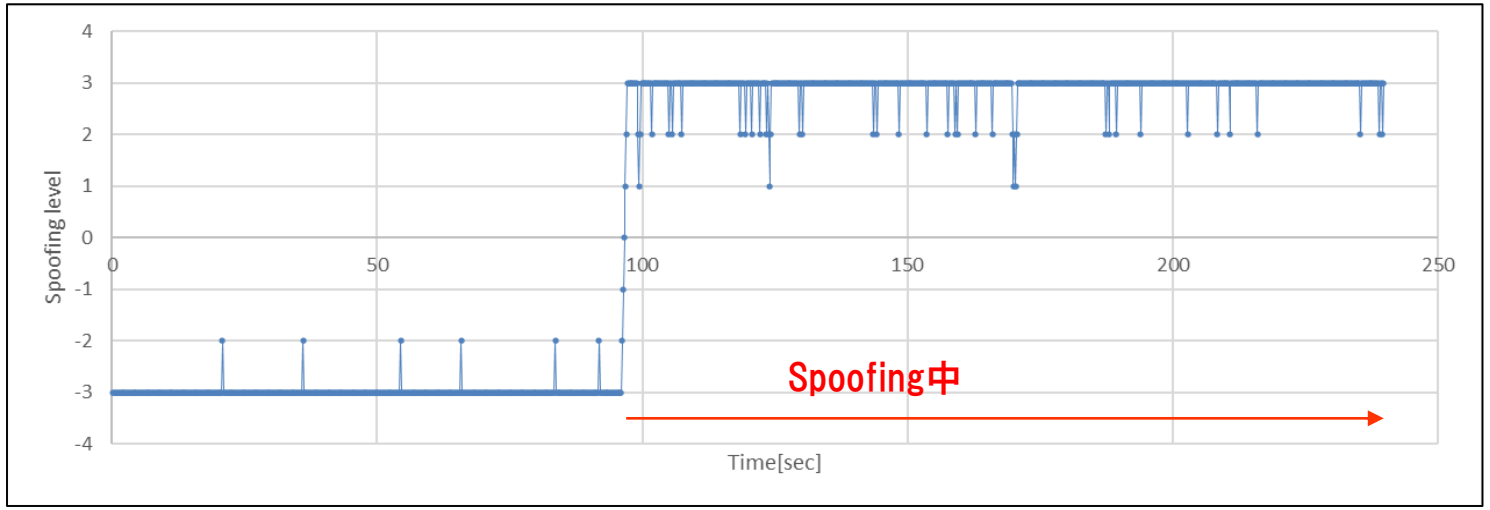
Spoofing flagの時系列グラフ

5. 評価実験1

マルチパスモニタリング
スプーフィング実験

Spoofing level使用した場合、0.6秒(3エポック)でSpoofing level≧0となりその後、Spoofing levelが0未満に落ちることはなかった。

	スプーフィングなし		スプーフィング中	
Total epoch	450	100.0%	450	100.0%
Spoofing flag=true	5	0.7%	422	93.8%
Spoofing flag=false	445	98.9%	28	6.2%

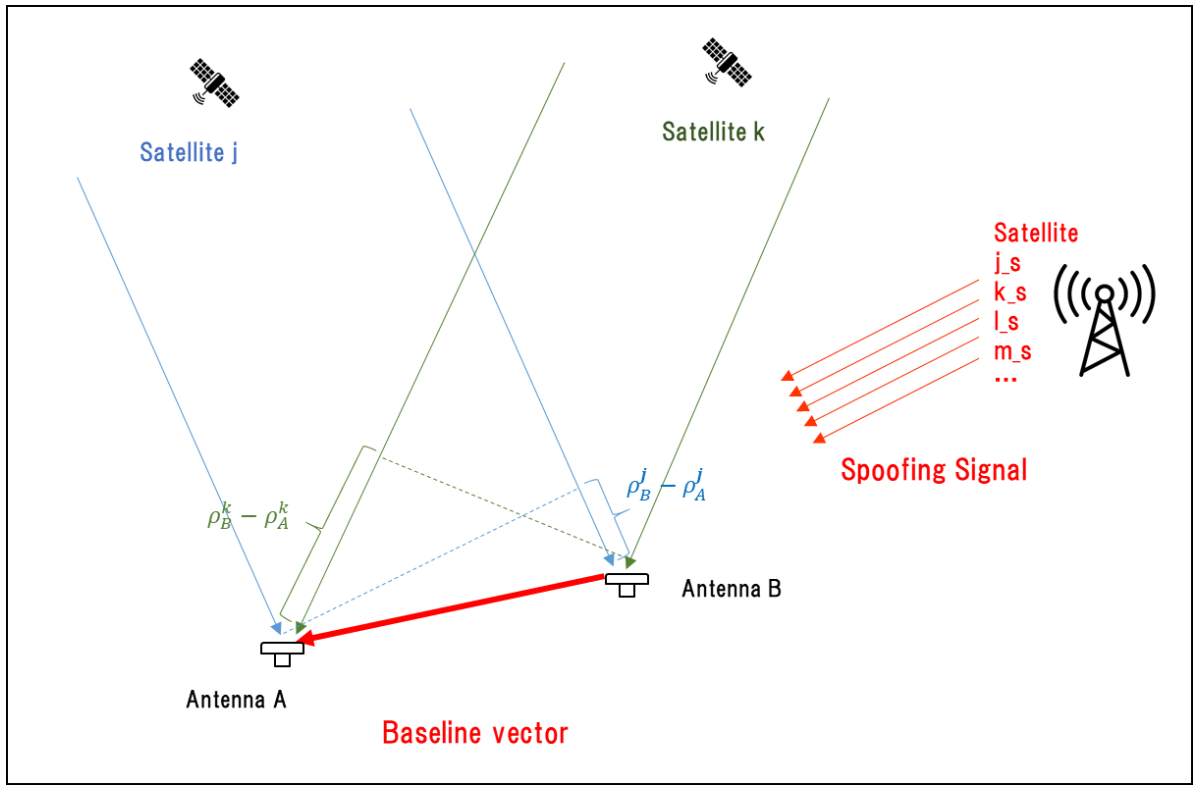


Spoofing level の時系列グラフ

6. 基線長解析によるスプーフィング検知手法

2つの距離を離したアンテナで同じ衛星の信号を観測したときの搬送波位相の差に注目した。

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0となる。



基線ベクトルの計算には以下の二重位相差を用いる。

$$\varphi_{AB}^{jk}[cycle] = \varphi_{AB}^{k} - \varphi_{AB}^{j}$$

$$= \left(\rho_B^k - \rho_A^k - (\rho_B^j - \rho_A^j)\right) \cdot \frac{f}{c} + \mathrm{N}_{AB}^{jk}$$

スプーフィング中は

$$\left(\rho_B^k - \rho_A^k - (\rho_B^j - \rho_A^j)\right) = 0$$

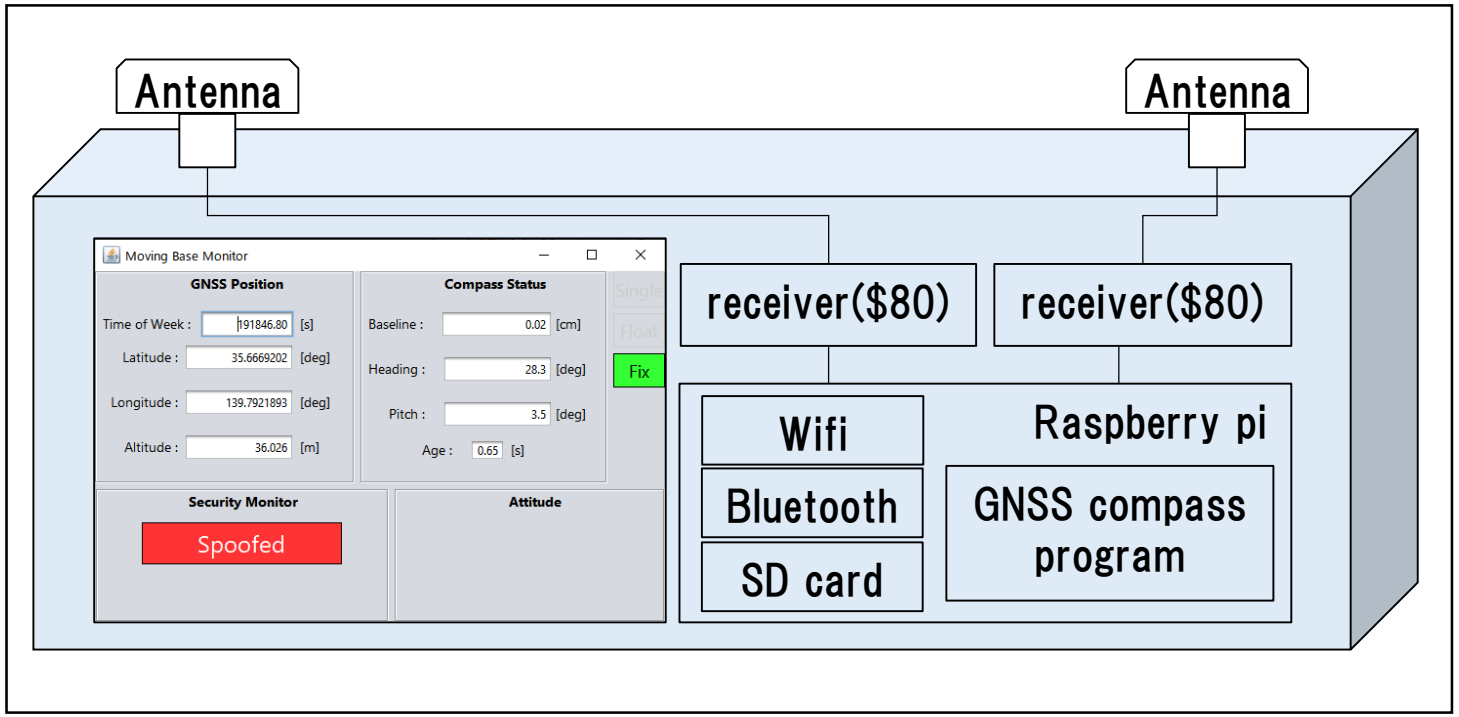
となるため、バイアス値のみ残り、ベクトルの大きさが0になる。

6. 基線長解析によるスプーフィング検知手法

Moving-base RTKはアンテナ間の精密なベクトルを求めることができるので、方位センサーとして船舶では広く使用されている。

本研究では市販受信機とラズベリーパイを使用してこの方位センサーを自作し、それにスプーフィング検知機能を付属させた。

＊KODEN KGC-300



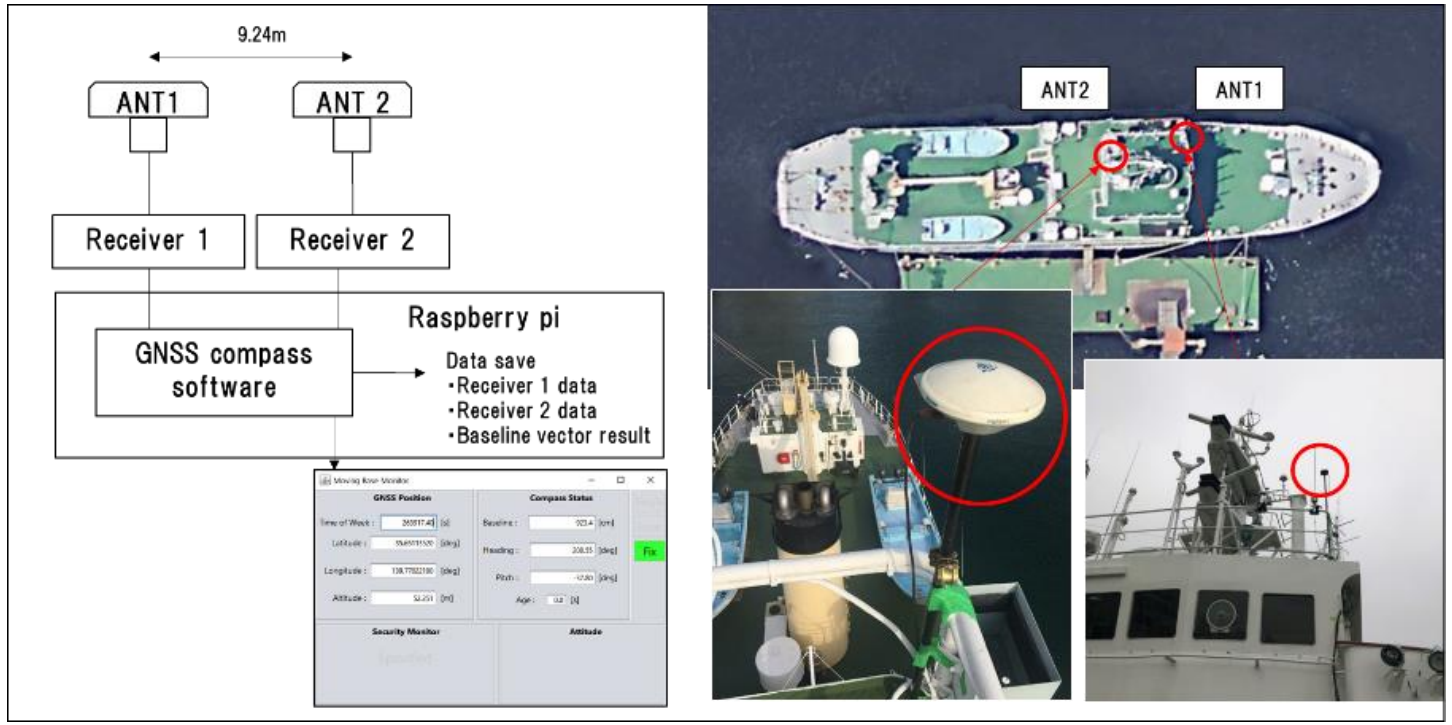
スプーフィング機能付きGNSSコンパスの構成

7. 評価実験2

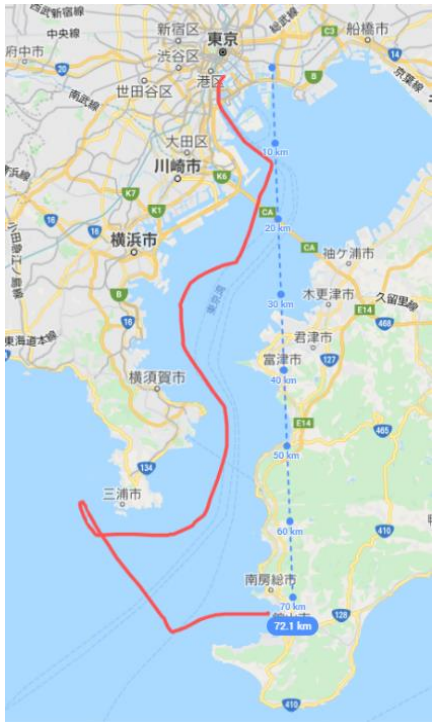
基線長解析
船上実験

自作装置を使用してそのアベイラビリティと誤検出率がないかを船上実験で評価した。

2020/01/15 汐路丸にて実験航海中、6時間のデータを取得。



実験構成図



航路

7. 評価実験2

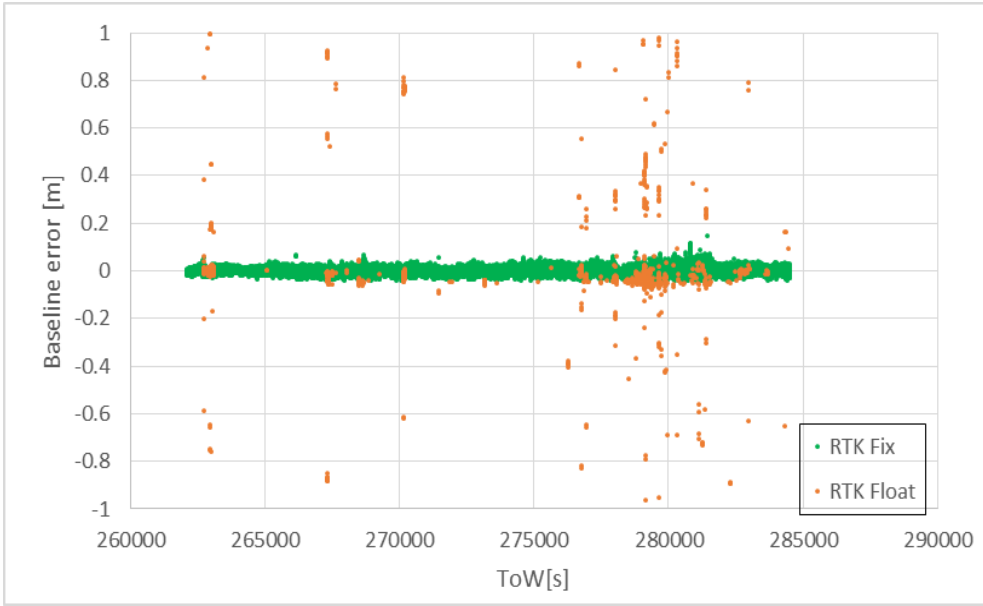
基線長解析
船上実験

基線長解析によるスプーフィング検知手法ではGNSSの信号環境が悪い等で基線ベクトルの計算ができないと判定ができない。(アベイラビリティ)

本実験でのアベイラビリティは98.18%でそのうち基線ベクトルが5cm以下となった誤検出は0%であった。

	Epoch	Percentage		
RTK Fix	106039	98.18%	Miss Fix	0.10%
			Spoofing false detection	0.00%
RTK Float	1759	1.63%	Miss Fix	50.14%
			Spoofing false detection	0.00%
No result	202	0.19%	–	–
Total	108000	100.00%	–	–

実験結果



正しいアンテナ間距離と比較した計算結果の誤差

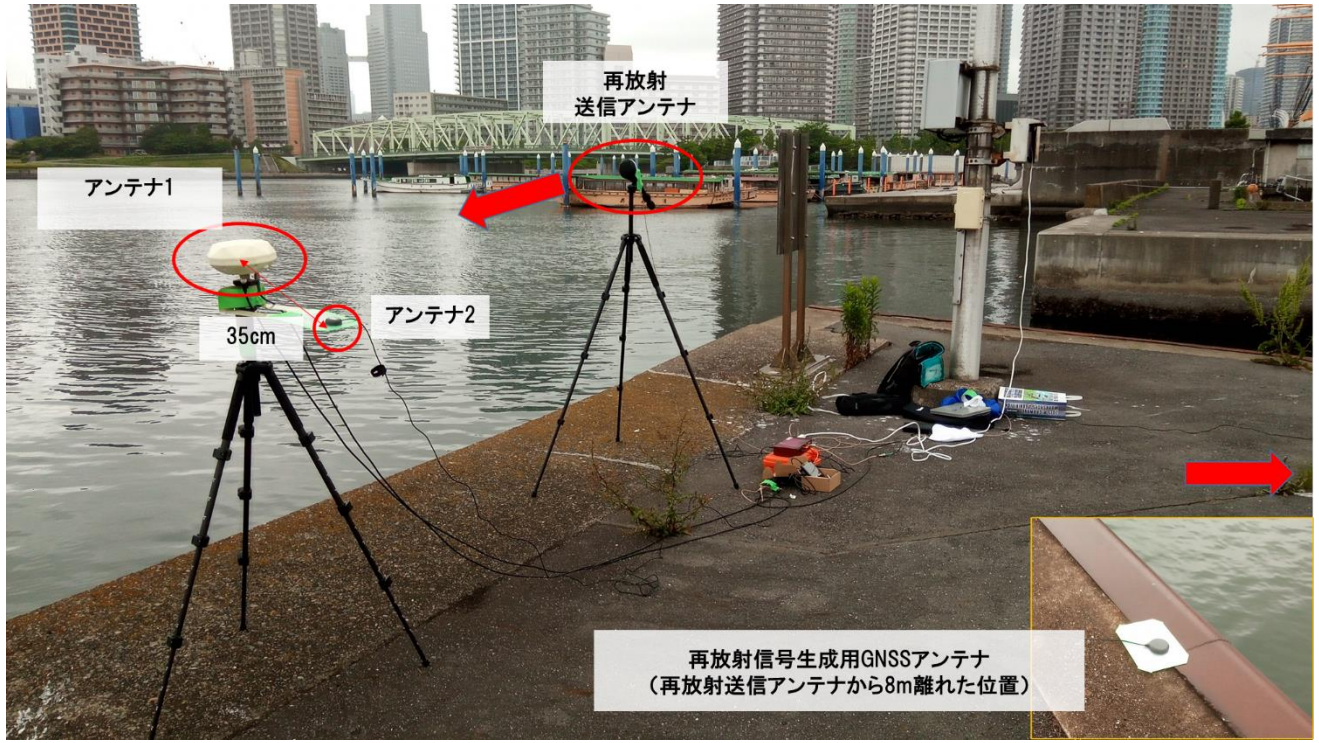
7. 評価実験2

基線長解析
スプーフィング実験

基線長解析によるスプーフィング検知手法の見逃し率をスプーフィング実験で確認した。

2020/05/22 東京海洋大学越中島キャンパスポンドにてスプーフィングを行いそのデータを取得。

スプーフィングは3mの距離から再放射を利用して再現した。

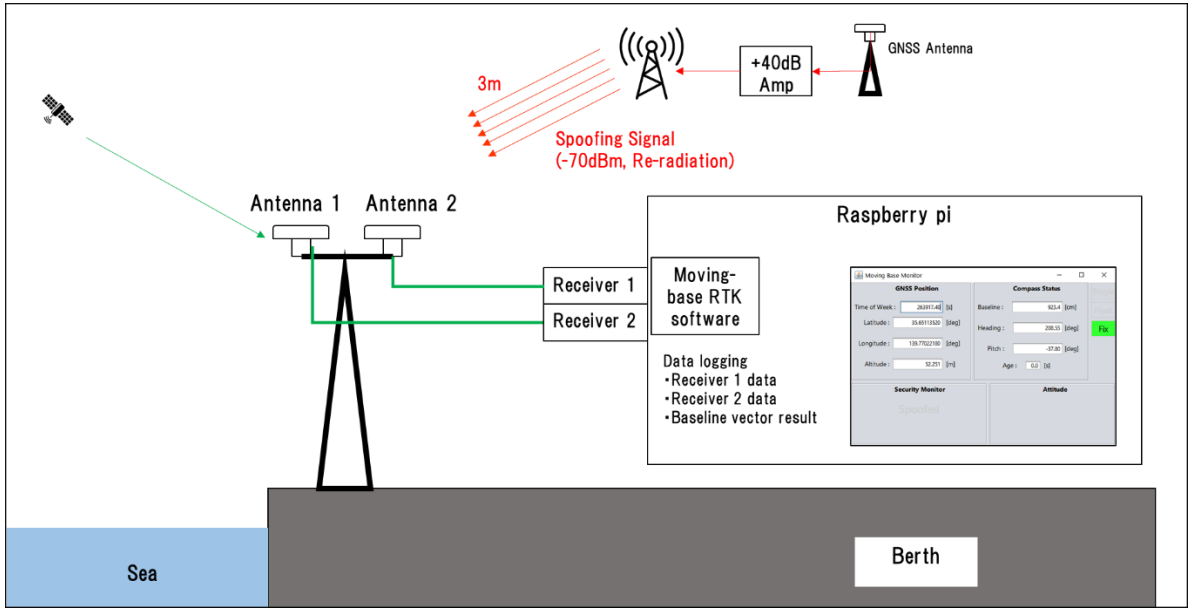


実験環境

7. 評価実験2

基線長解析
スプーフィング実験

実験機材はアンテナ、受信機以外船上実験で使用したものと同じものを利用した。



実験環境

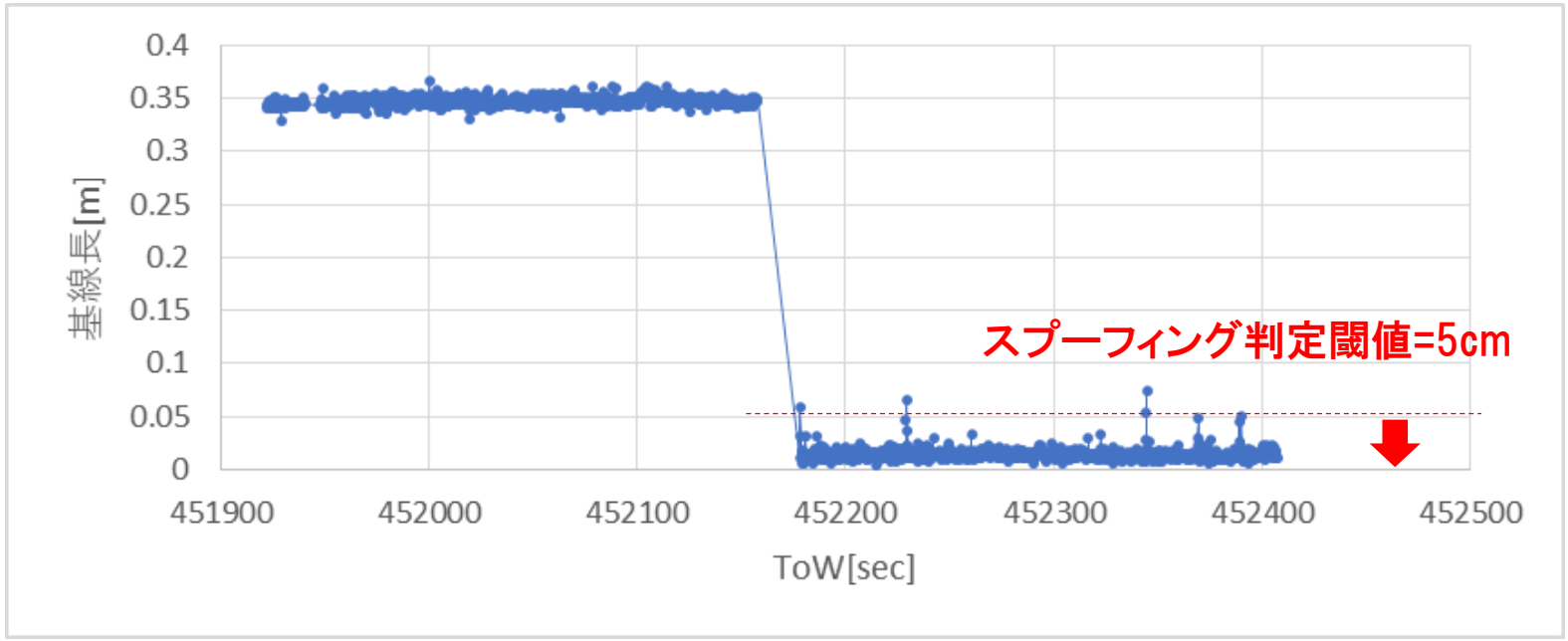
実験機材

名称	メーカー/型番	説明
アンテナ1	FANTASTIC project (RHCPアンテナのみ使用)	RHCPとLHCPの2偏波アンテナ L1,L2,L5 帯 LNA 38dB
アンテナ2	Tallysman TW4722	L1帯 マルチGNSS LNA 23dB
受信機1	ublox M8T	L1帯1周波 GPS+BDS+Galileo+QZSS 5HzでRawデータ出力
受信機2	ublox M8T	L1帯1周波 GPS+BDS+Galileo+QZSS 5HzでRawデータ出力
Moving-baseRTKソフトウェア	–	L1帯1周波 GPS+BDS+Galileo+QZSS
再放射アンテナ	GPS source GNSS-3P	L1,L2,L5 帯パッシブアンテナ
再放射用アンプ	mini-circuit ZX60-2534MA	500MHz-2500MHz 1.5GHzで+39.4dB
再放射信号生成用アンテナ	Tallysman TW4722	L1帯 マルチGNSS LNA 23dB

7. 評価実験2

基線長解析
スプーフィング実験

基線長の変化からスプーフィングが発生したことが確認できた。



スプーフィング前後の基線長の変化

7. 評価実験2

基線長解析
スプーフィング実験

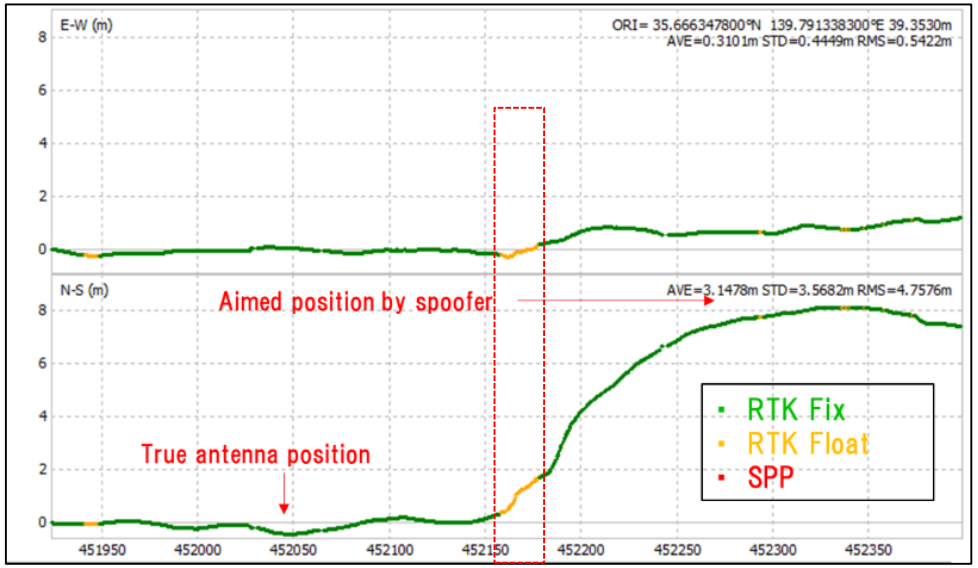
スプーフィング開始後248.8秒間の検知結果はアベイラビリティが88.42%、そのうち見逃しが0.45%であった。

主にスプーフィング開始後の20秒間ほどでベクトル計算ができなかった。

これは受信機が完全にスプーフィング信号を追尾するまで時間がかかるため。

	Epoch	Percentage		
RTK Fix	1100	88.42%	baseline < 0.05	99.55%
			baseline ≧ 0.05	0.45%
RTK Float	129	10.37%	baseline < 0.05	52.71%
			baseline ≧ 0.05	47.29%
No result	15	1.21%	-	-
Total	1244	100.00%	-	-

実験結果



スプーフィングによる緯度経度の変化と、RTKステータス

8. まとめ

◆船舶において他者からのスプーフィング攻撃を検知する手法を2つ提案した。

◆検知即応性とコンパクト性では**マルチパスモニタリング手法**に、
コストとシステムの簡便性では**基線長解析手法**にそれぞれ利点がある。

◆どちらの手法でも1%未満のスプーフィング誤検出率、見逃し率を確認できた。

<今後の課題>

◆移動体が遠距離からスプーフィング攻撃を受けた環境での評価を行う。

◆検知後に継続して自身のPVTを得るためのGNSSに代替する測位手法の研究を行う。