Spoofing Detection on Ships Using Multipath Monitoring and Moving-baseline Analysis

ION2020+, 23 Sept 2020

Kaito Kobayashi, Nobuaki Kubo
Tokyo University of Marine Science and Technology

Contents

1. GNSS use on ship

A lot of marine electronic devices depend on PVT information from GNSS.

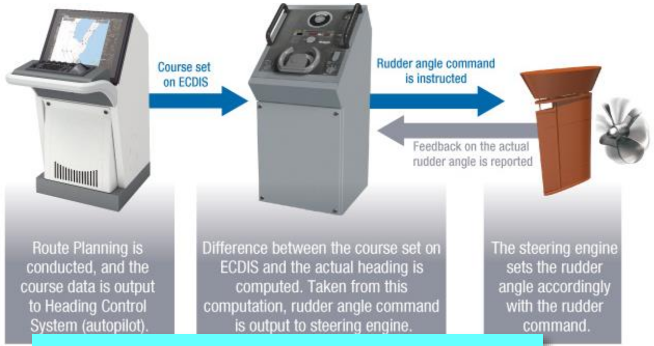
GNSS

PVT

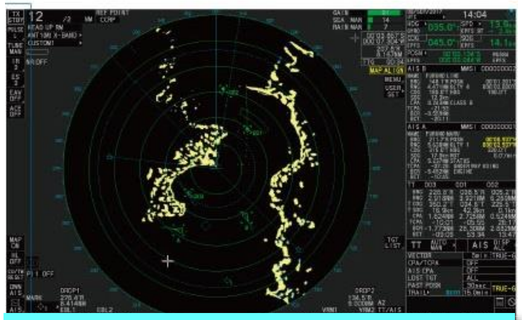
Speed, Course, Attitude

ECDIS

AIS



Auto Pilot



Radar

Satellite communication

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

1. GNSS use on ship

In the future…

Remote ship operation, Auto berthing

↓

more precious and robust positioning
 will be required.

2. Motivation

However, due to a spread of GNSS spoofing technic, we should solve potential risk regarding GNSS on ship navigation.

$10,000

$200

Risk of low-cost spoofing device spread

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

Pirate attack risk

Running aground, Collision

2. Motivation

Which anti-spoofing method is suitable for ship…

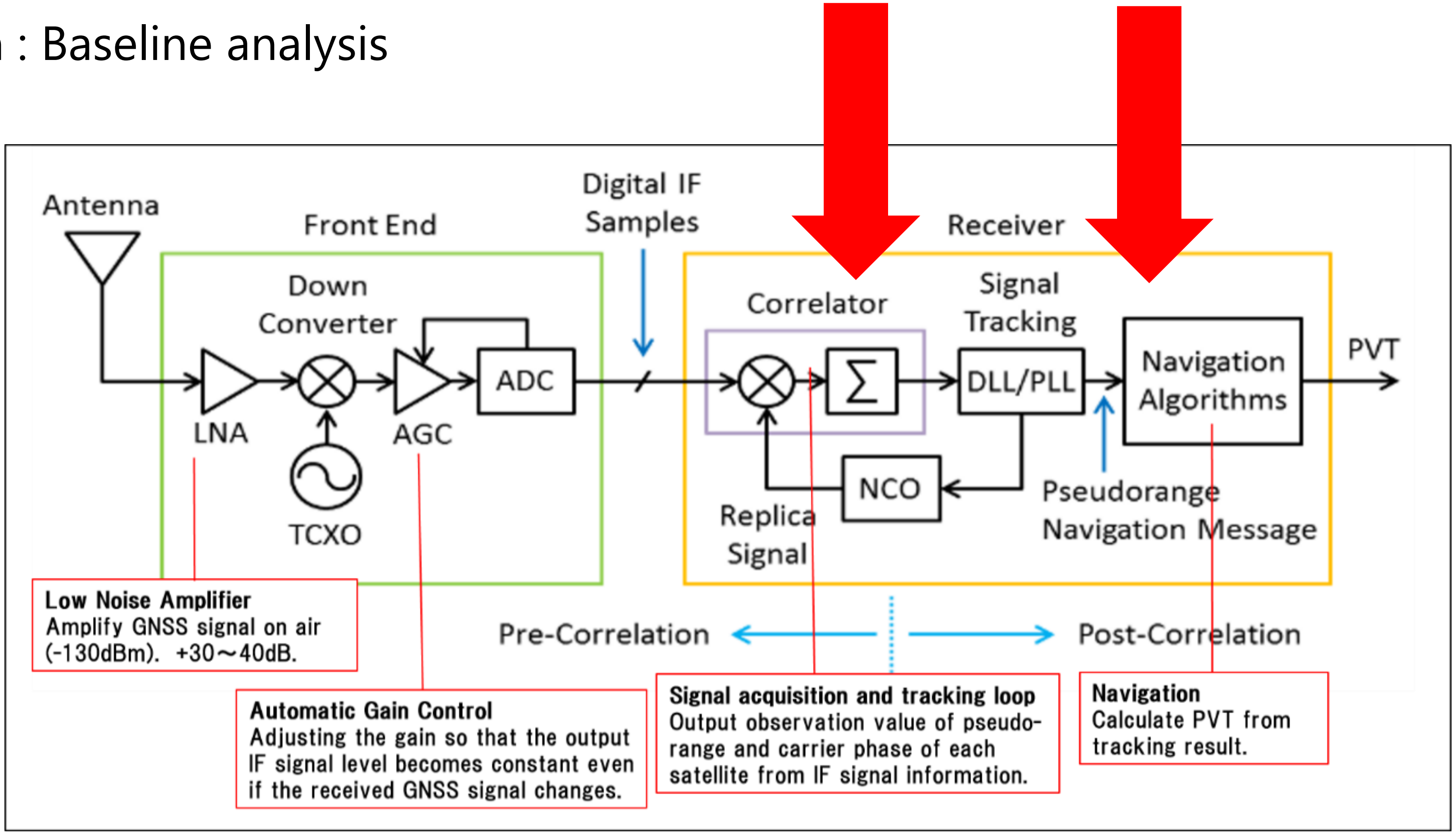
- **Use backup sensor**
  There is a lot of un-solved issue about sensor fusion on ship movement with roll and pitch. (IMU, Doppler sonar & Gyro compass, etc…)
- **Signal Authentication like NMA**
  Not effective for live GNSS signal re-radiation attack from coast or pirate ship.
- **GNSS receiver stand-alone**
  Difficult under non-open-sky environment.
  However on ship environment is mostly open-sky environment.

We propose spoofing detection method by GNSS receiver stand-alone focus on sea environment.

3. Overview of the proposed method

We proposed 2 methods for spoofing detection.

1. Pre-correlation : Multipath monitoring
2. Post-correlation : Baseline analysis



3. Overview of the proposed method

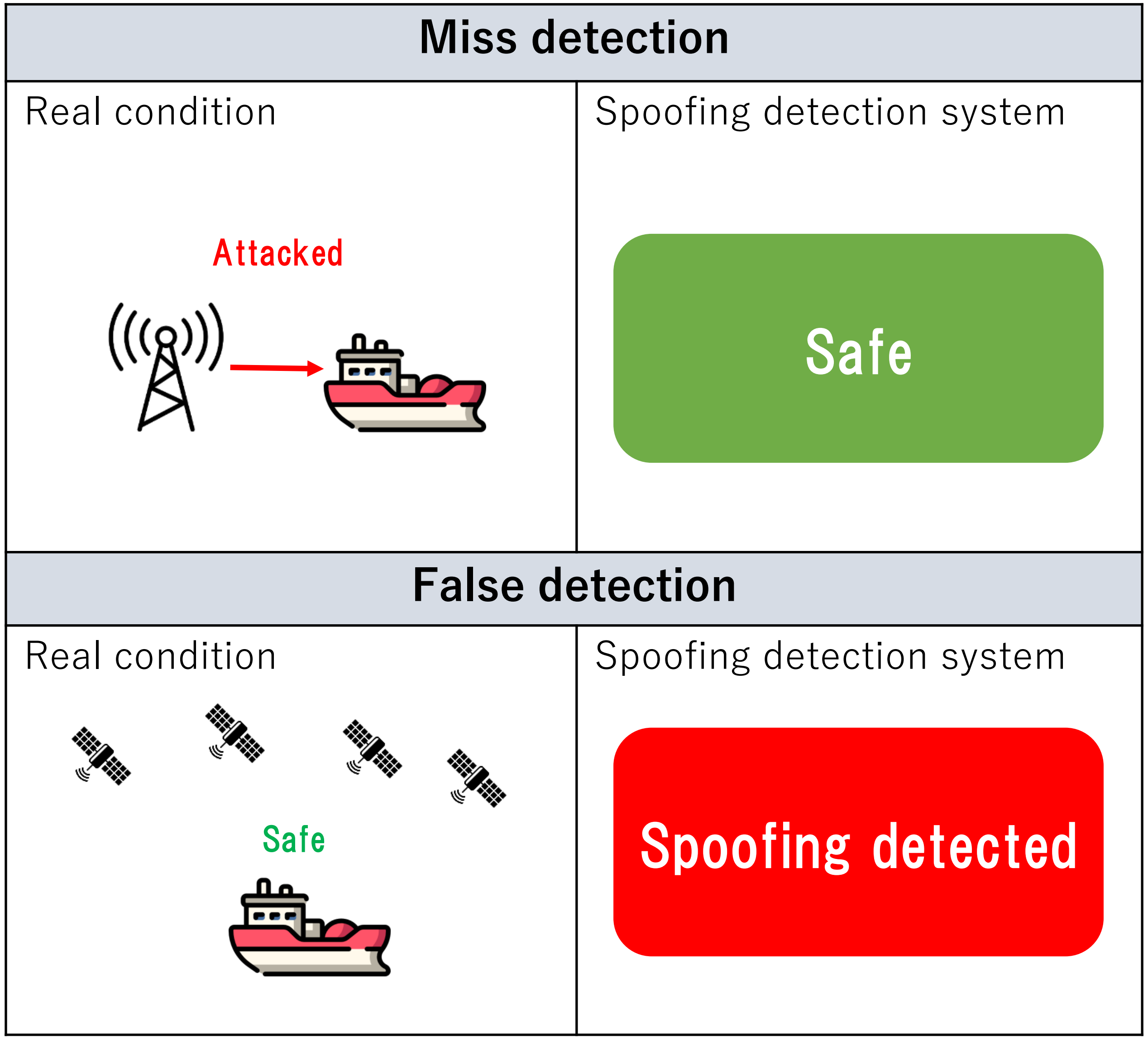
We combined 2 methods to aim for more robust spoofing detection.

“Robust” means reduction of miss detection and false detection.

Multipath Monitoring (Pre-correlation)

✖

Moving-baseline analysis (Post-correlation)

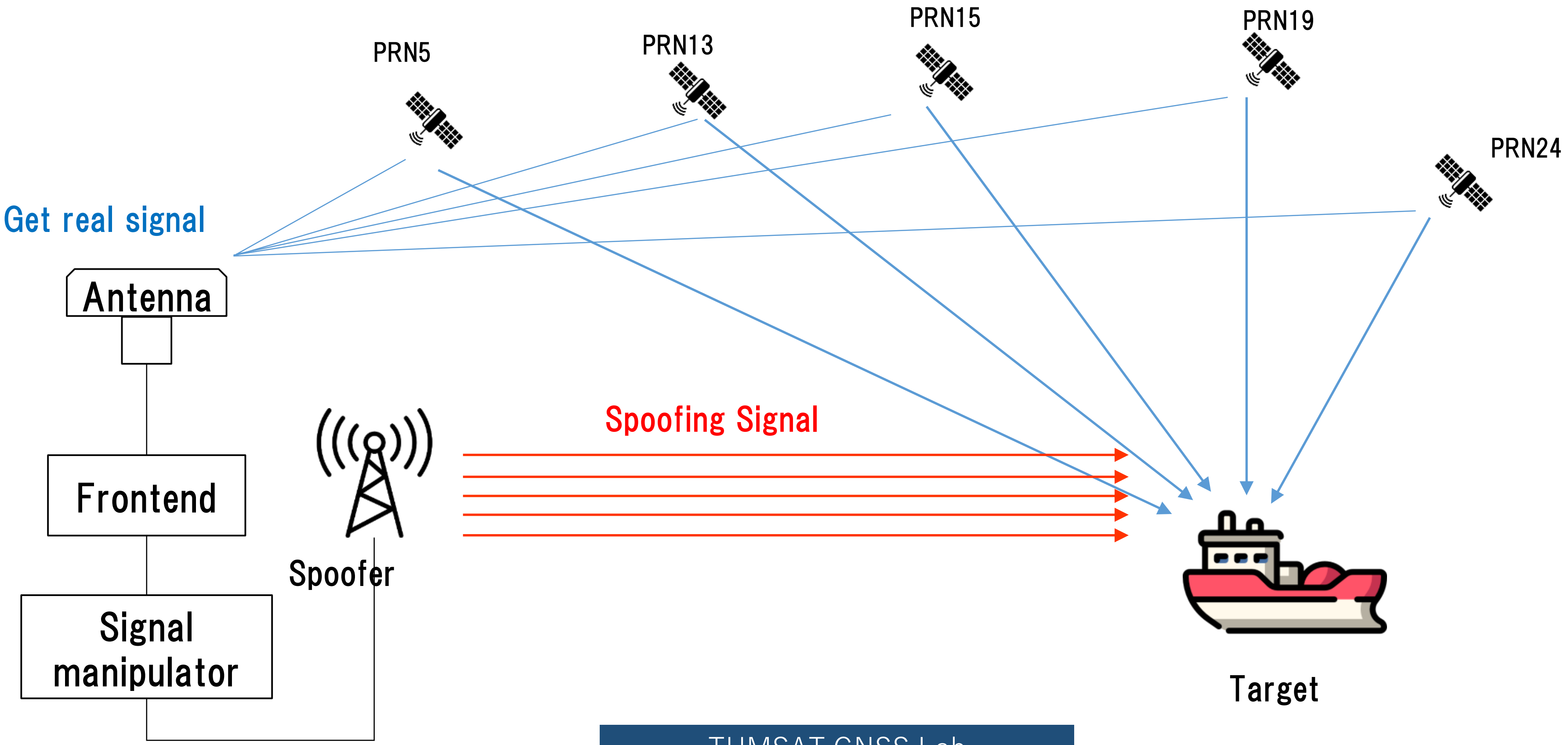


3. Overview of the proposed method

Both method focus on the spatial feature of GNSS signal path.

Spoofing signal arrives with same signal path for all satellites.

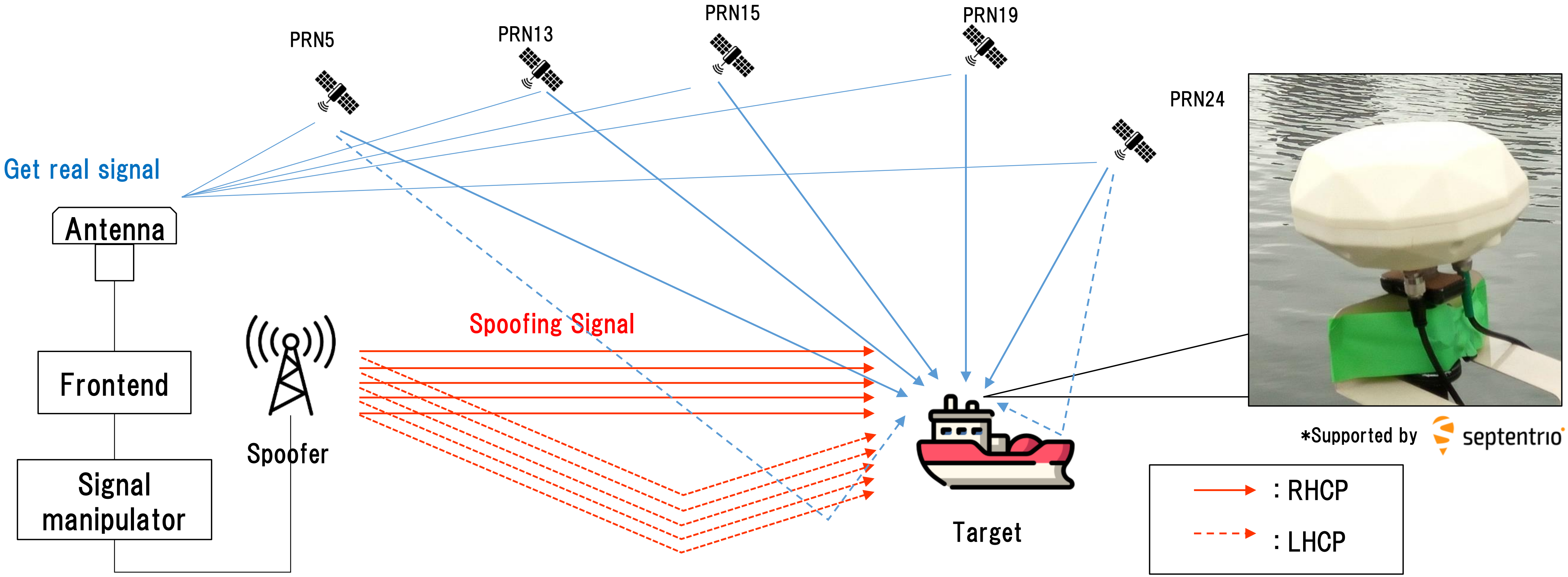
However, live GNSS signal path have diversity from satellite's position difference.



4. Multipath monitoring

We tracked both direct signal (RHCP) and multipath signal (LHCP) by dual polarization antenna.

On ship, multipath signals are mainly caused by sea reflection and their characteristic should be similar on all spoofing signal.



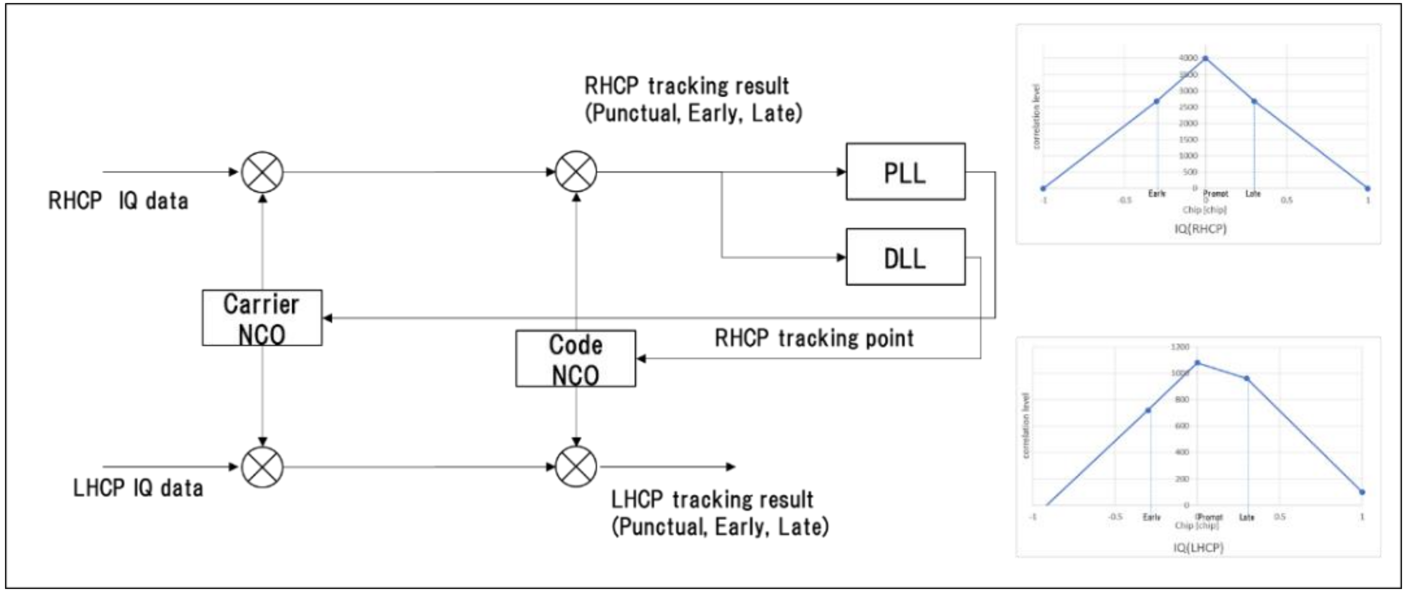
4. Multipath monitoring

We expressed multipath characteristic as 2 parameters.

$$\frac{\boldsymbol{R}}{\boldsymbol{L}}\textbf{Signal Ratio [dB]} = 20 \cdot \log 10 \cdot \left| \frac{\mathrm{Ip(R)} + \mathrm{i} \cdot \mathrm{Qp(R)}}{\mathrm{Ip(L)} + \mathrm{i} \cdot \mathrm{Qp(L)}} \right|$$

$$\frac{\boldsymbol{R}}{\boldsymbol{L}}\textbf{code delay } [\boldsymbol{degree}] = \arctan(\mathrm{a}, \mathrm{b}) \qquad \left(\frac{\mathrm{Ip(R)}+\mathrm{i}\cdot\mathrm{Qp(R)}}{\mathrm{Ip(L)}+\mathrm{i}\cdot\mathrm{Qp(L)}} = a + i \cdot b\right)$$

RHCP and LHCP signal which received on dual polarization antenna are tracked in parallel and 2 parameters are estimated in each satellites.



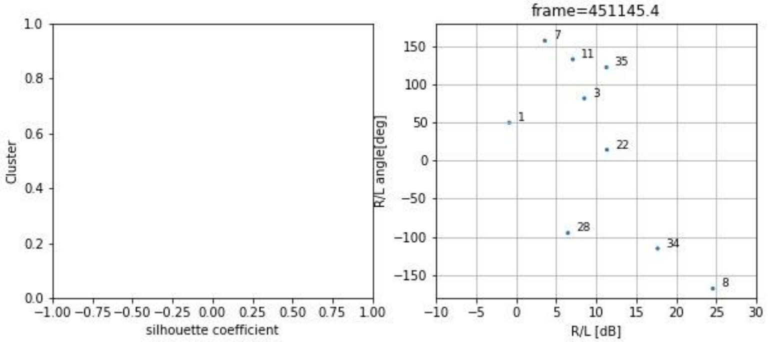
Ip : Prompt correlation value of I phase
Qp : Prompt correlation value of Q phase
(R) : RHCP signal
(L) : LHCP signal

4. Multipath monitoring

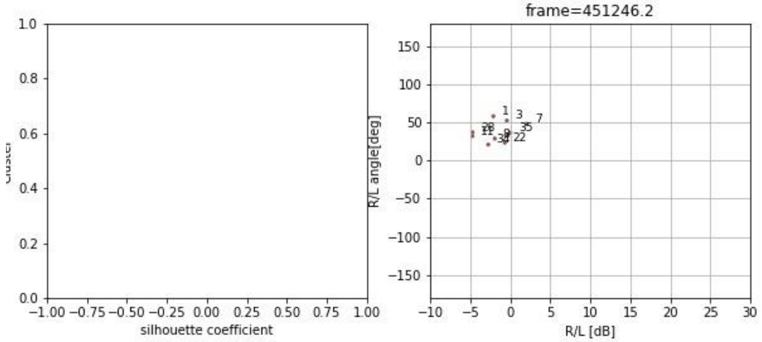
When these 2 parameters are plotted, multipath affinity between satellites are represented as dense cluster.

This cluster is consisted by spoofing satellite signals.

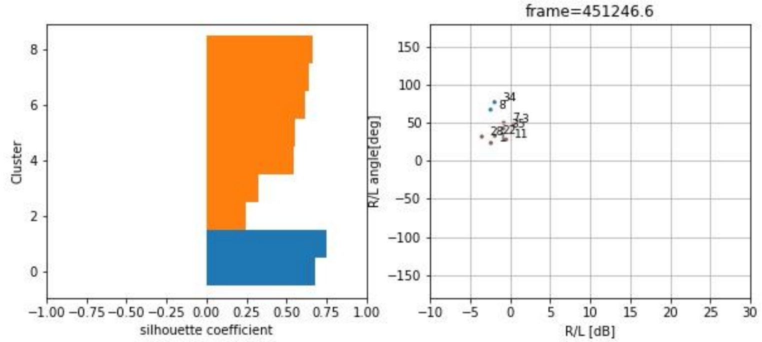
We identify this cluster by DBSCAN clustering algorithm and silhouette analysis.



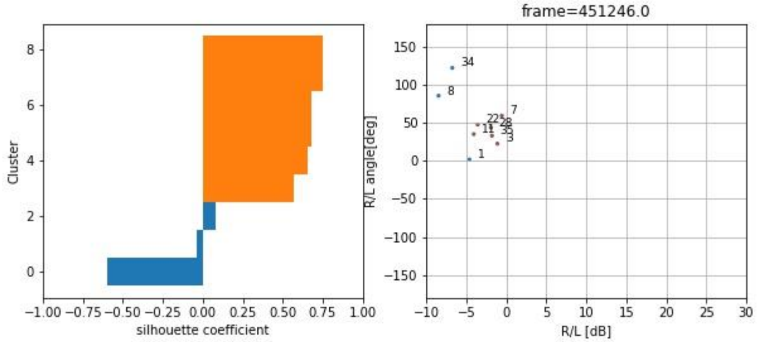
All live satellites
(Noise cluster)



All satellites are spoofed
(1 cluster)



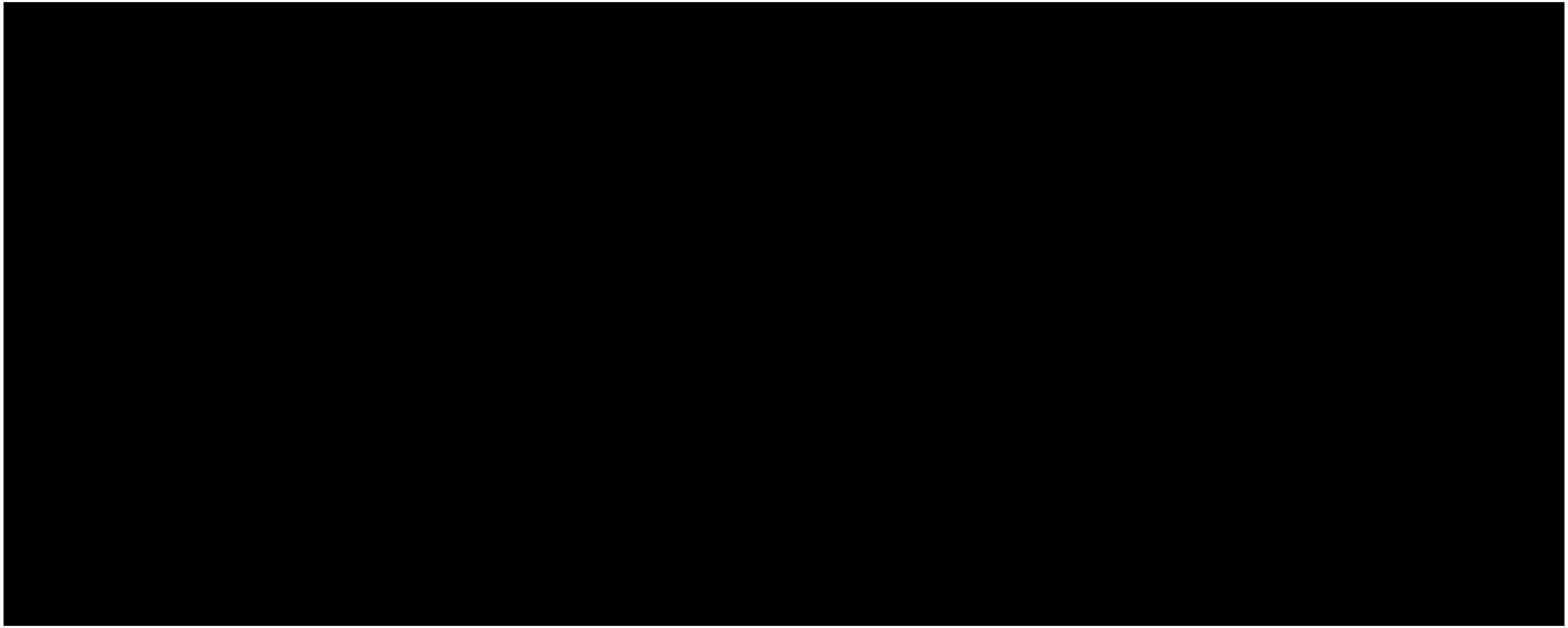
All satellites are spoofed
(2 cluster appears)



6 spoofed satellites and 3 live satellites
(1 cluster and 1 noise cluster)

4. Multipath monitoring

Example of non-spoofing and spoofing.

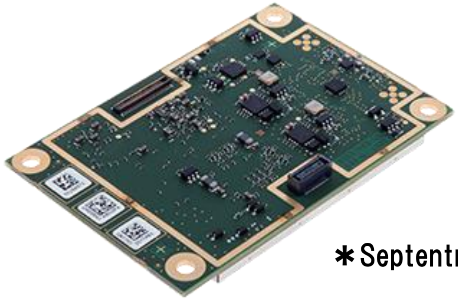


5. Moving-baseline analysis

We focused on the carrier range double difference between 2 antennas.

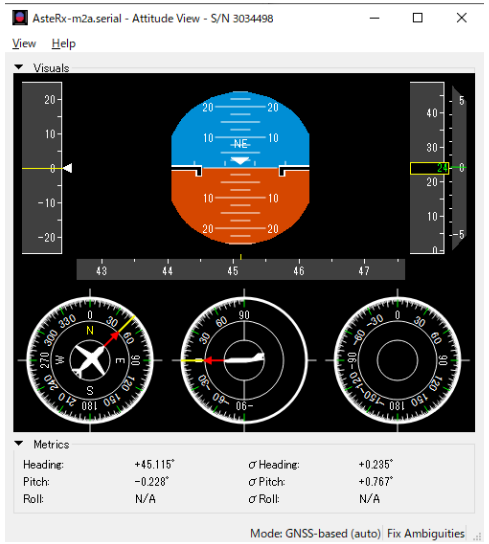
Base algorithm is moving-base RTK which calculate base line vector.
This is already used as a GNSS compass on ship for heading sensor.

＊FURUNO SCX-20



＊Septentrio AsteRx-m2a

＊KODEN KGC-300

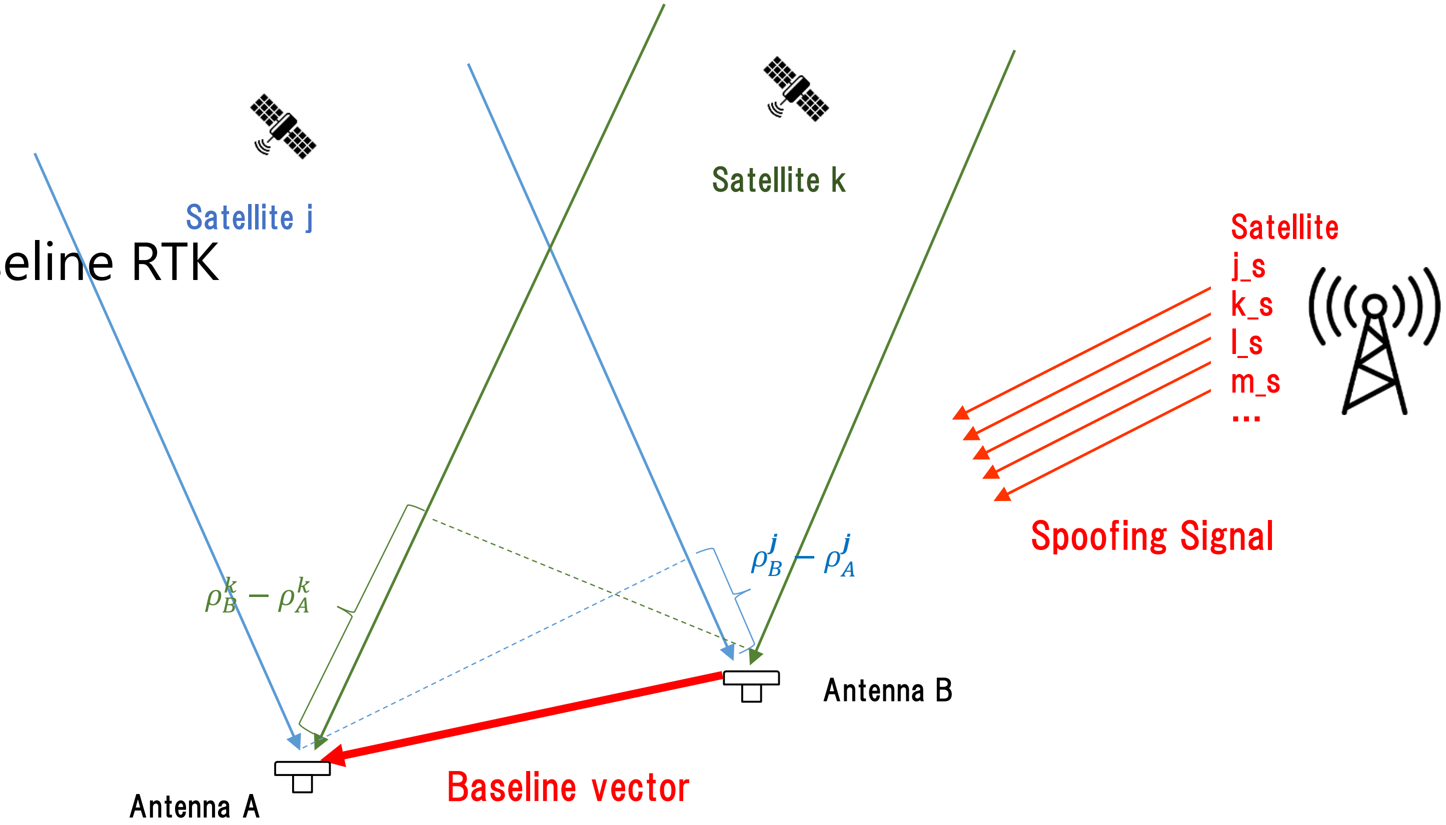


5. Moving-baseline analysis

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

When both A and B track spoofing signal, $\rho_B^{k\_s} - \rho_A^{k\_s}$ and $\rho_B^{j\_s} - \rho_A^{j\_s}$ becomes same value because the arrival direction of spoofing signal is same for satellites j_s and k_s

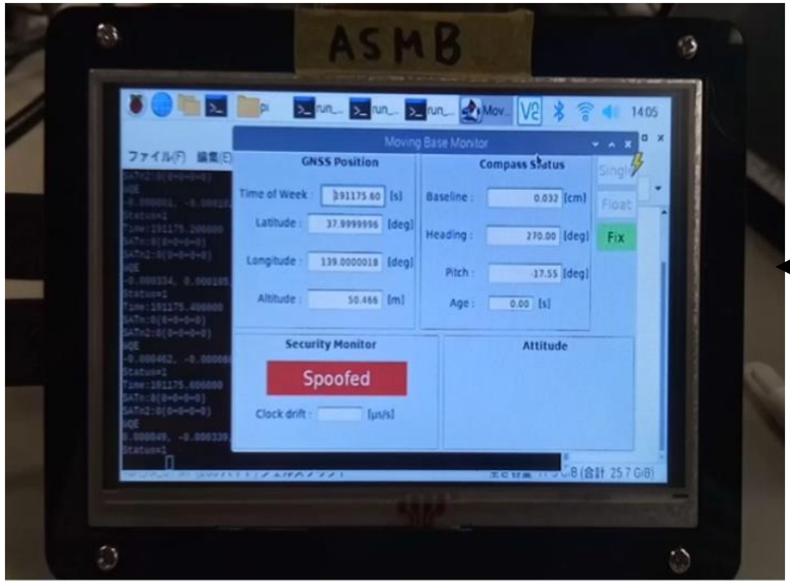
$(\rho_B^k - \rho_A^k - (\rho_B^j - \rho_A^j))=0$ means zero baseline RTK and baseline length become 0.



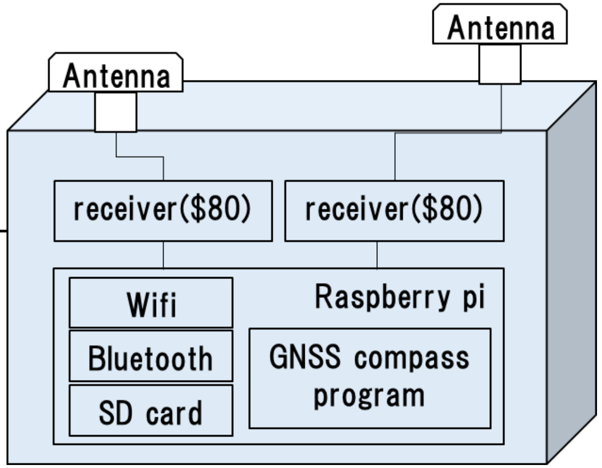
5. Moving-baseline analysis

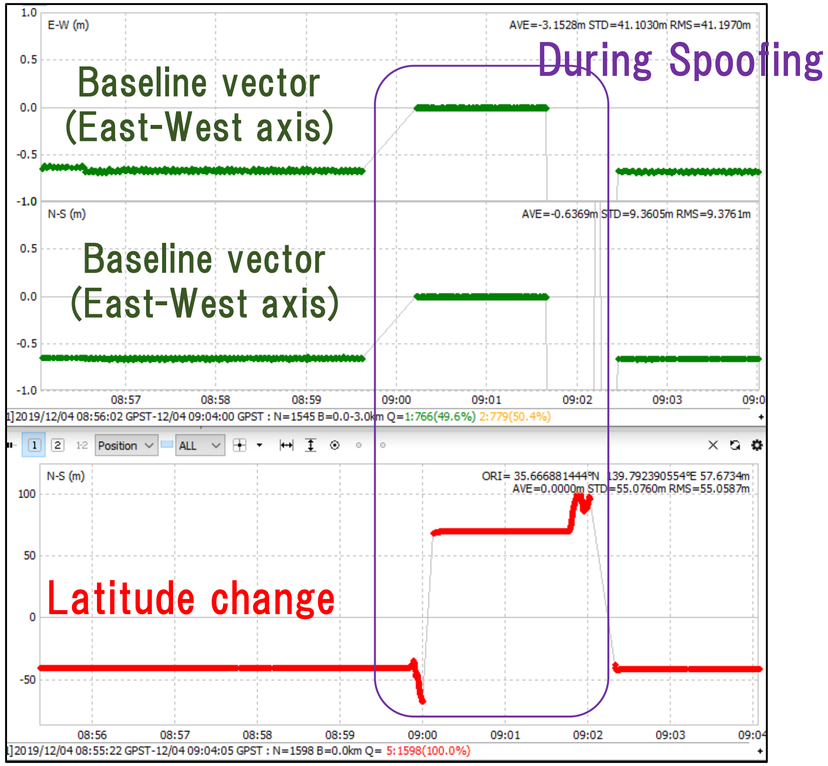
We developed GNSS compass includes spoofing detection alert.

The system supports consumer receiver that output raw observation (ublox, septentrio, etc…) and moving-base RTK engine support GPS, Galileo, BDS, QZSS L1 band.



Monitor

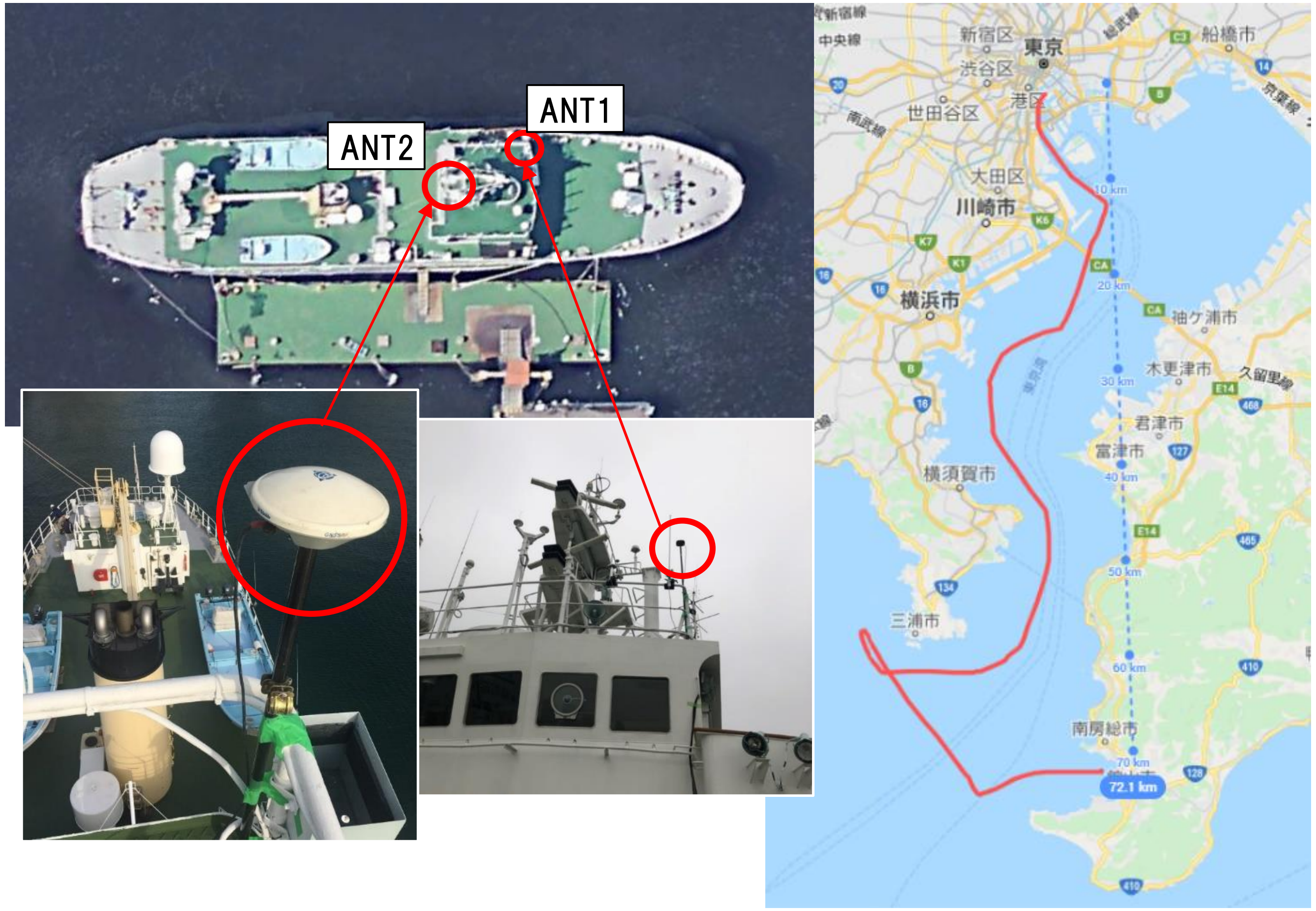




5. Moving-baseline analysis

Availability of the spoofing detection by moving-baseline analysis depends on fix rate of moving-base RTK.

We evaluated it on 6 hours ship voyage.



Name	Manufacturer	Detail
Antenna 1	Trimble Zephyr2 Rover	L1,L2,L5 band LNA 50dB
Antenna 2	JAVAD GrAnt−G5T	L1,L2,L5 band LNA 32dB
Receiver 1	ublox ZED−F9P	Dual Frequency GPS+GLONASS+BDS+Galileo+QZSS 5Hz interval raw data output
Receiver 2	ublox ZED−F9P	Dual Frequency GPS+GLONASS+BDS+Galileo+QZSS 5Hz interval raw data output
Moving−baseRTK sofrware	−	Single Freaquency GPS+BDS+Galileo+QZSS

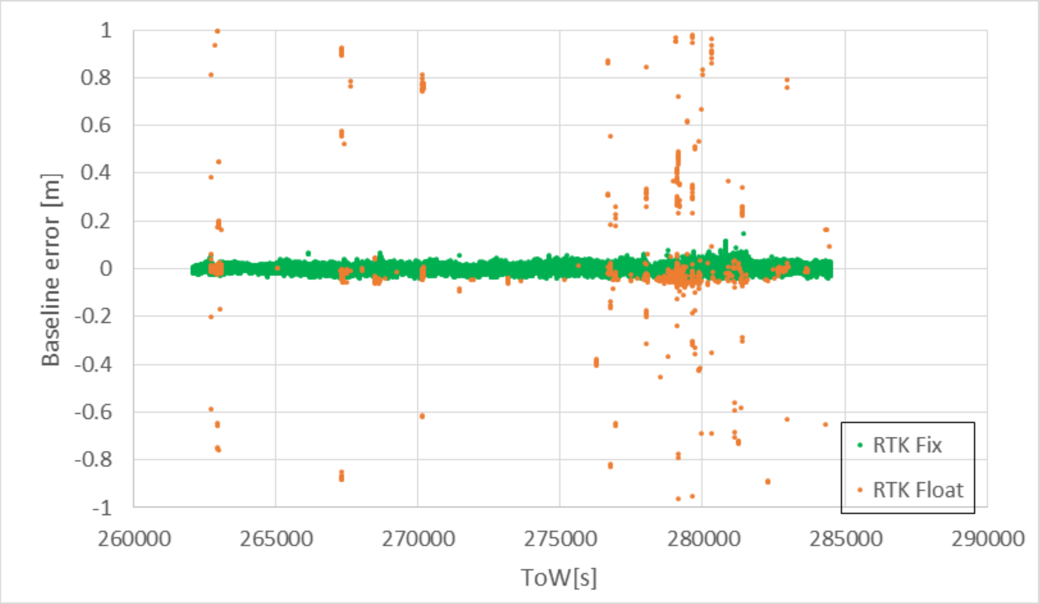
Experimental devices

5. Moving-baseline analysis

The result of moving-base RTK on ship

Availability of the system while voyage was 98% and false detection was not appeared.

- Float solution has some error about baseline length and it can't be used for spoofing detection judgment

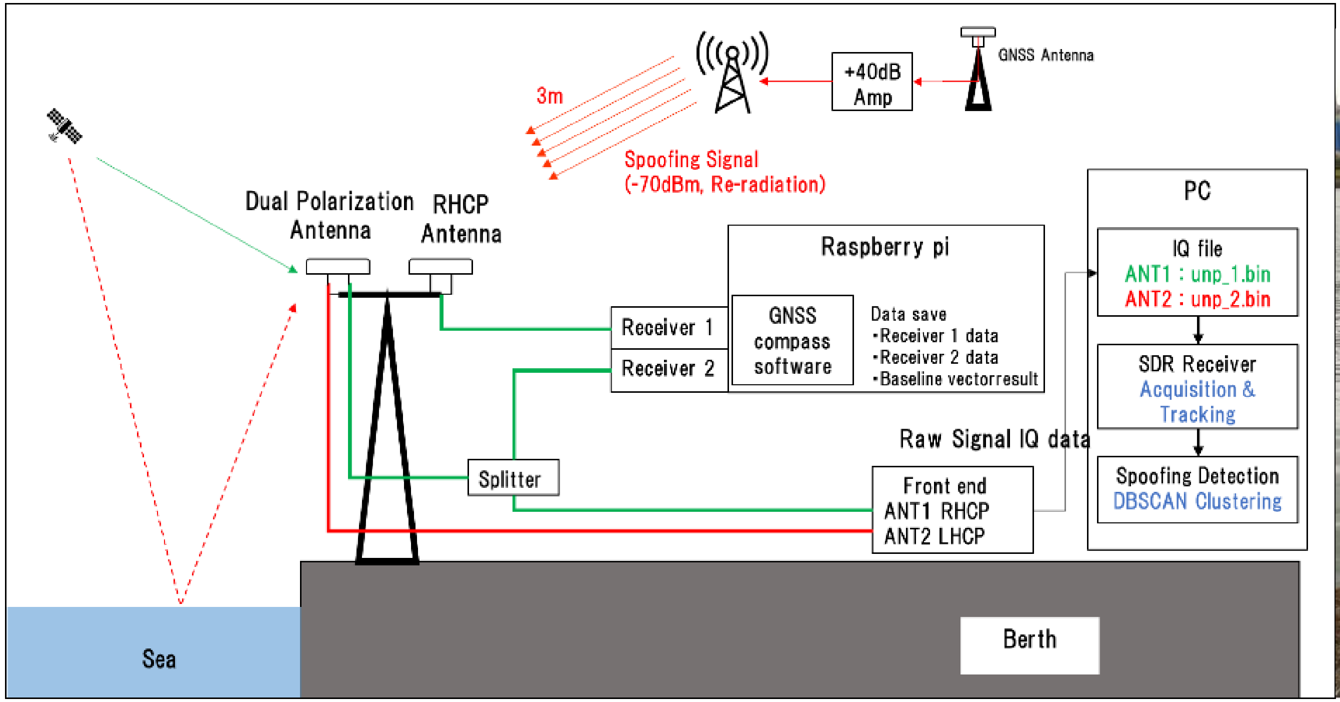


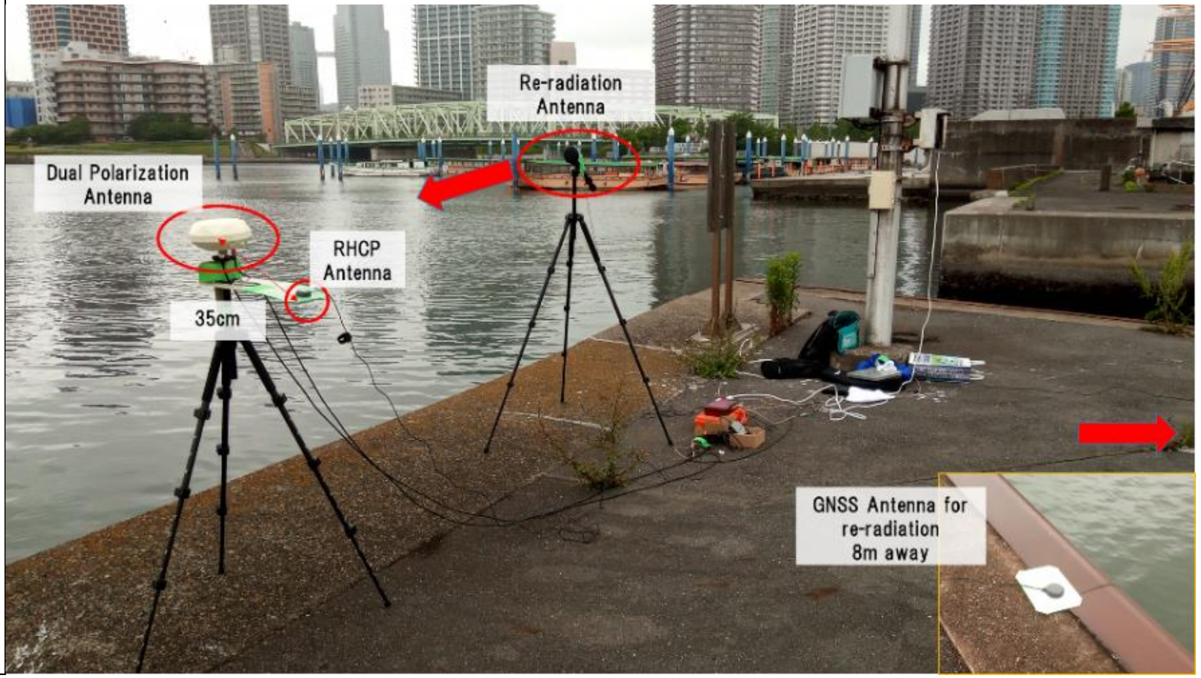
	Epoch	Percentage		
RTK Fix	106039	98.18%	Miss Fix	0.10%
			Spoofing false detection	0.00%
RTK Float	1759	1.63%	Miss Fix	50.14%
			Spoofing false detection	0.00%
No result	202	0.19%	–	–
Total	108000	100.00%	–	–

6. Experiment

We evaluated both method simultaneously under live GNSS signal contaminated by spoofing signal.

*This experiment was planned to conduct on ship but impossible by COVID19.

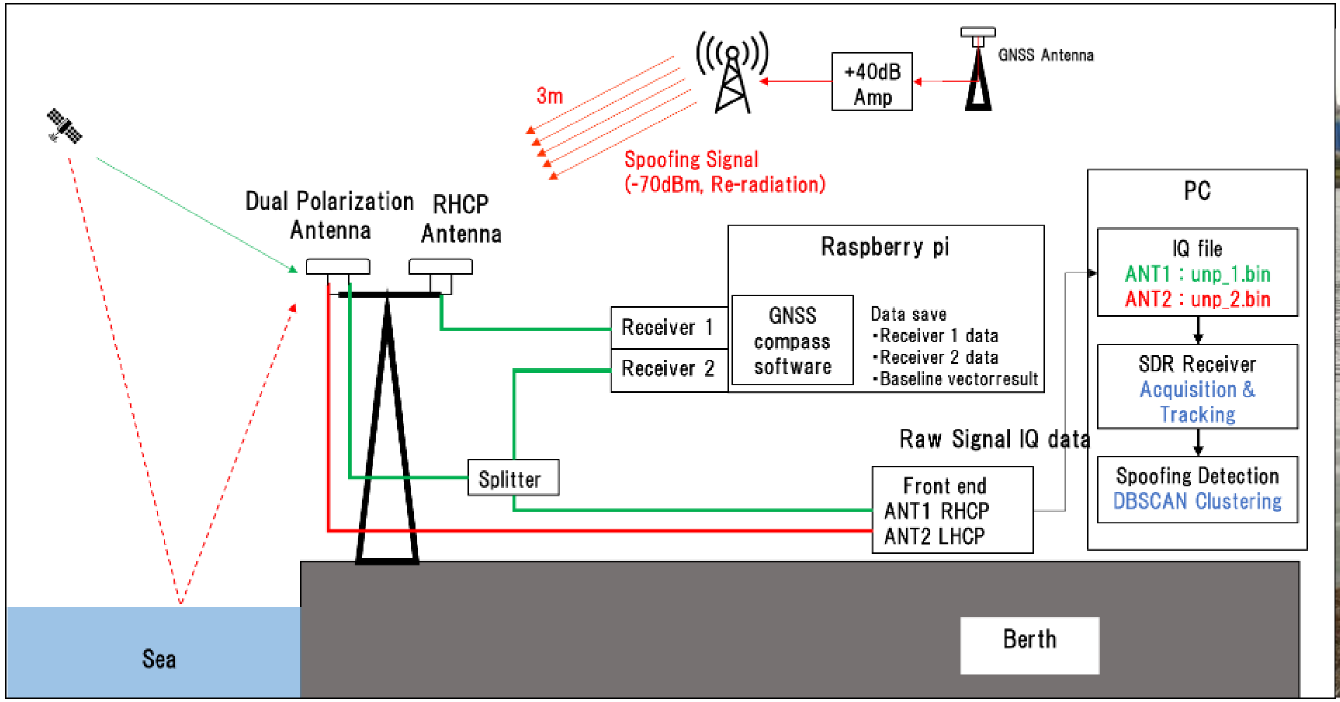


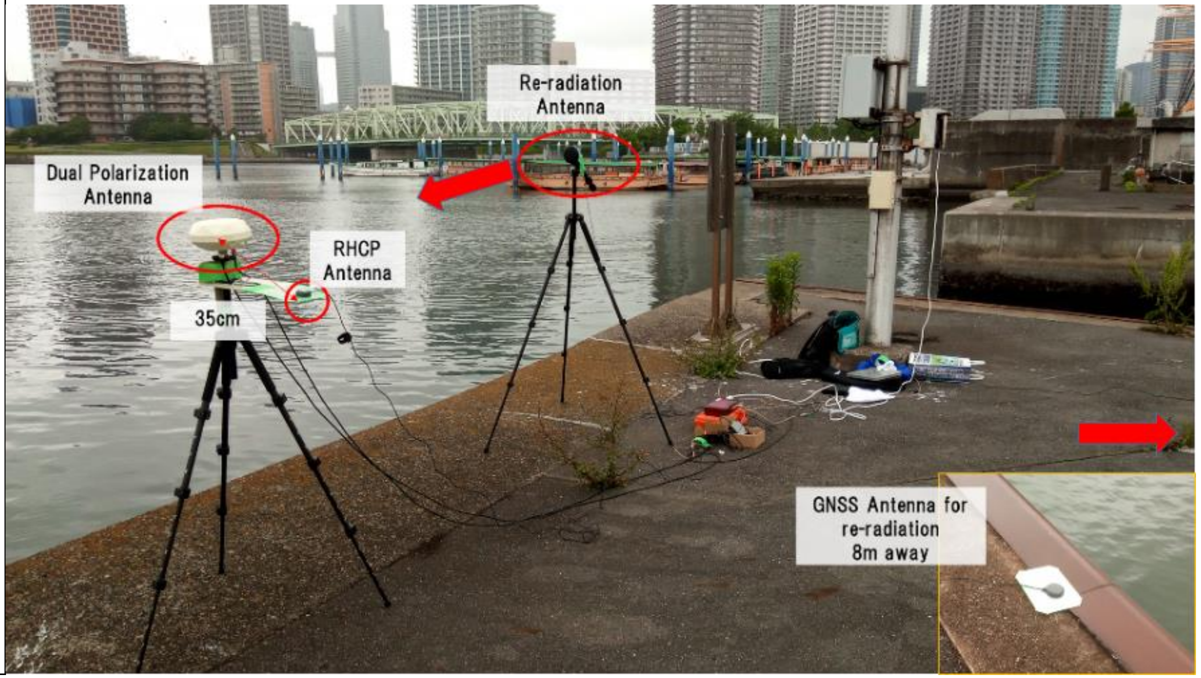


6. Experiment

Spoofing was conducted by re-radiation of live GNSS signal received at another location.

After 90 sec non-spoofing, we start spoofing for 150 sec. Data was analyzed by 5 Hz.

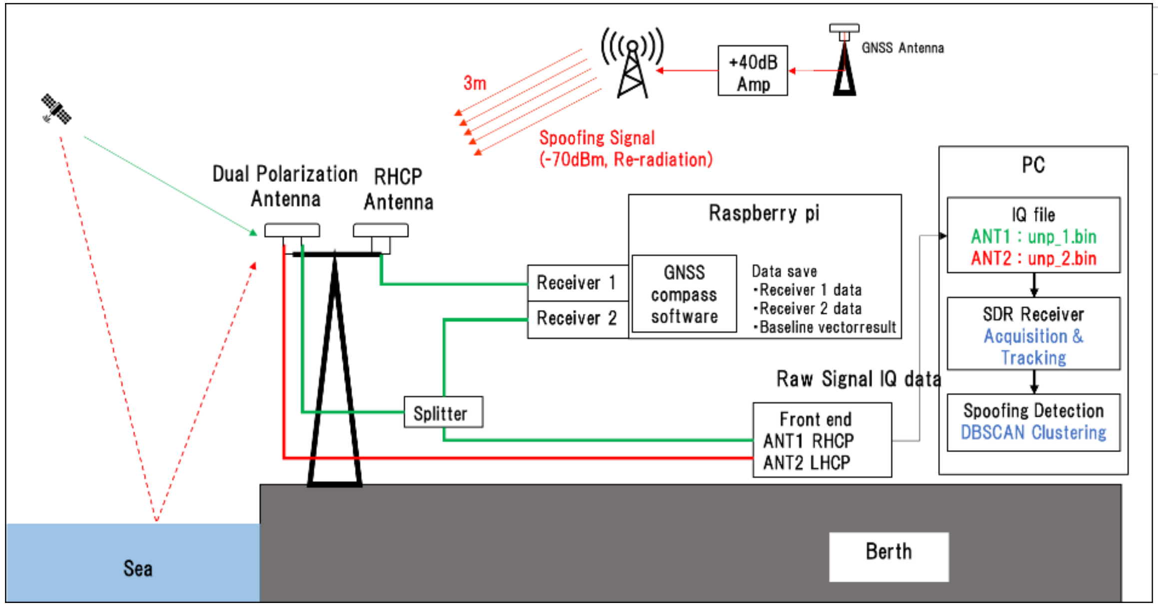




6. Experiment

Name	Manufacturer	Detail
Dual Polarization Antenna	FANTASTIC project	Dual-polarization of RHCP and LHCP L1,L2,L5 band LNA 38dB
RHCP Antenna	Tallysman TW4722	L1band multi GNSS LNA 23dB
Front end	IP Solution	Dual channel input Frequency=1575.42MHz IF=4.092MHz Sampling rate=16.368MHz 2bit IQ sampling
SDR GNSS Receiver	–	Dual channel input GPS L1C/A, QZSS L1C/A

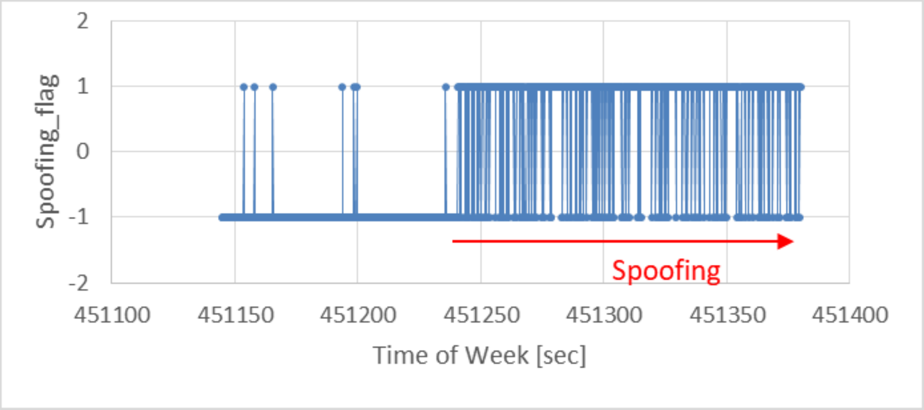
Name	Manufacturer	Detail
Receiver 1	ublox M8T	Single Frequency GPS+BDS+Galileo+QZSS 5Hz interval raw data output
Receiver 2	ublox M8T	Single Frequency GPS+BDS+Galileo+QZSS 5Hz interval raw data output
Moving-base RTK sofrware	–	Single Freaquency GPS+BDS+Galileo+QZSS
Re-radiation Antenna	GPS source GNSS-3P	L1,L2,L5 band passive antenna
Amplifier for re-radiation	mini-circuit ZX60-2534MA	500MHz-2500MHz +39.4dB at 1.5GHz
GNSS Antenna for re-radiation	Tallysman TW4722	L1band multi GNSS LNA 23dB



6. Experiment

The result of the spoofing alert (Multipath monitoring method)

To eliminate a few epoch false detection or miss detection, we judged spoofing using time integration with limit.

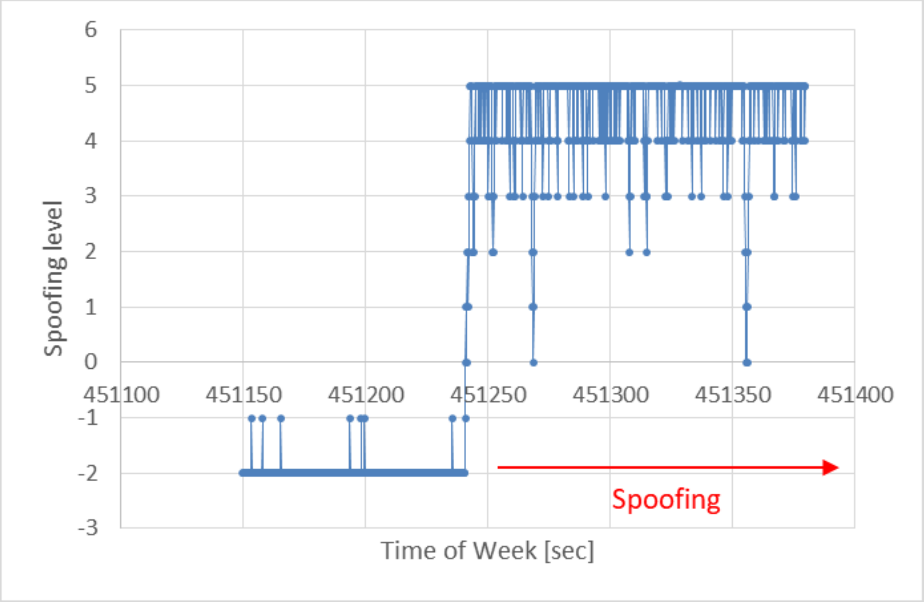


$$Spoofing\ level = \sum_{i=0}^{t} Spf_i \qquad (-2 \leq\ Spoofing\ level \leq 5)$$

Any spoofing cluster detected : Spf=1

No spoofing cluster detected : Spf=-1

Spoofing level >0 : Spoofing



Only 2 epoch miss detection happens.

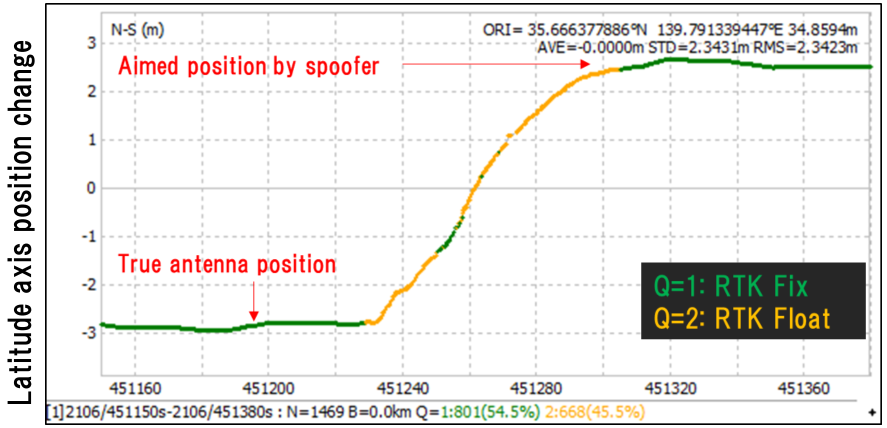
6. Experiment

The result of the spoofing alert (Moving-baseline analysis)

Spoofing flag=0 : RTK fix and baseline > 5 cm

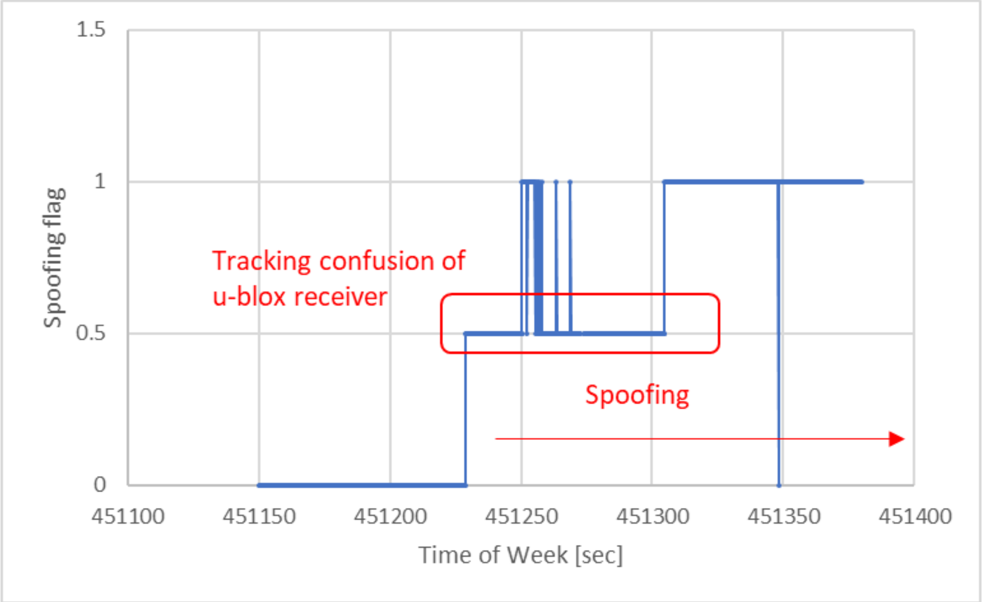
Spoofing flag =0.5 : RTK float, can't judge spoofing

Spoofing flag =1 : RTK fix and baseline <5 cm



By the tracking confusion of the receiver, it need a 77 sec until continuous spoofing detection.

Only one epoch miss detection (baseline length=5.02 cm)



7. Conclusion

2 spoofing detection methods for maritime use was evaluated

- ◆Both methods can achieve 0% false detection, and low rate miss detection.
- ◆"Multipath monitoring" has high sensitivity for spoofing (Fast detection) but it is unstable depends on multipath environment.
- ◆"Moving-baseline analysis" has better detection stability in perfect spoofing condition but it can't detect spoofing in imperfect spoofing condition (while receiver's tracking is confusing)

Combination of pre-correlation and post-correlation spoofing detection method will complement each other's shortcomings.