GNSS spoofing detection using two receivers in a very short baseline

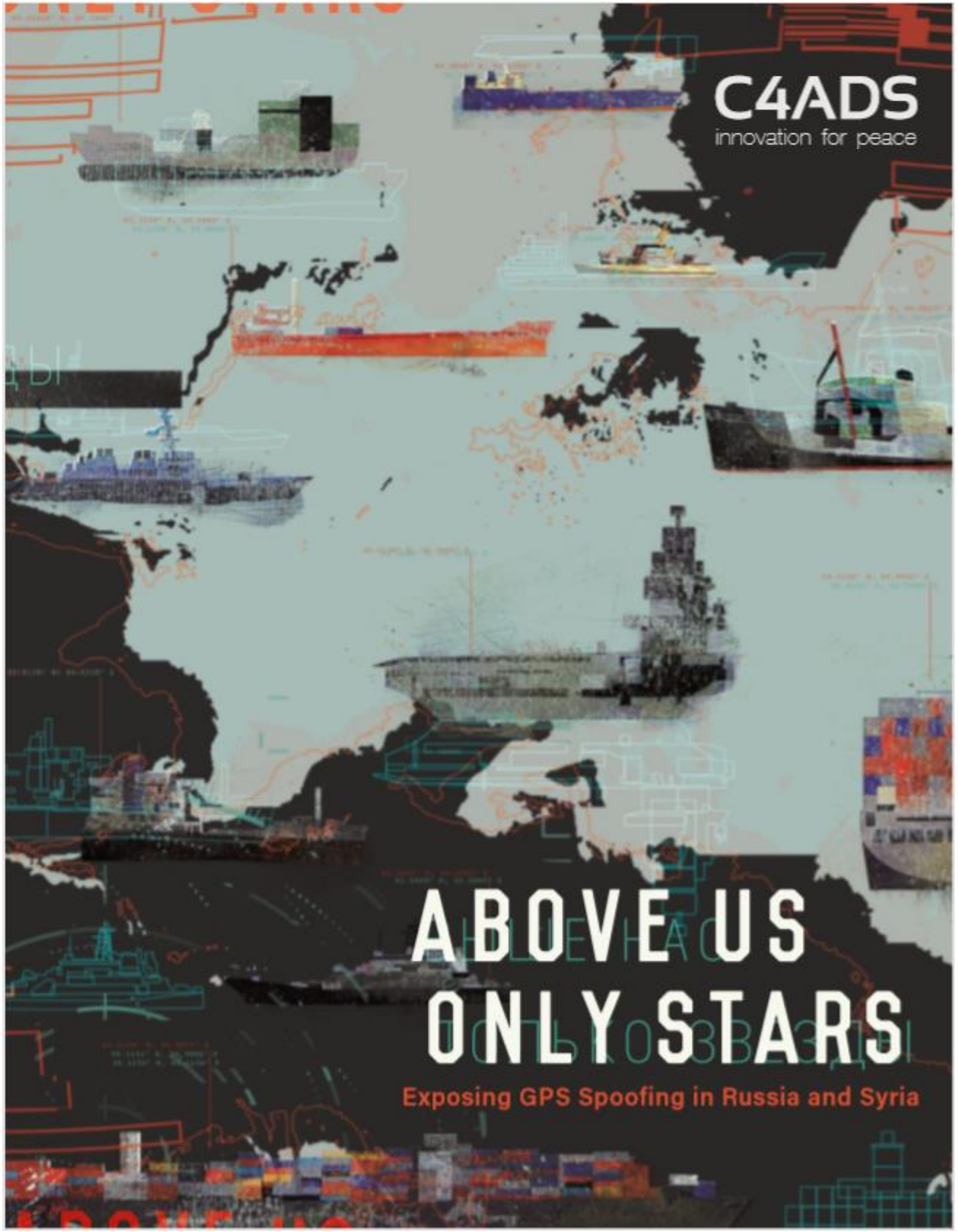
Barend Lubbers
Ghislaine Haggenburg
Homayoun Nikookar

International Navigation Conference 2019, Edinburgh
21 November 2019

Netherlands Defence Academy

Introduction

- GNSS Spoofing: realistic threat
- Not only state actors, also terrorist groups or criminals may spoof GNSS => Danger for both military and civil society
- Spoofing detection to increase integrity
- BSc. Thesis on spoofing detection using commercial off the shelve GNSS receivers



Research questions/objectives

- Is it possible to detect spoofing without knowing or estimating the baseline orientation?
- If possible, what are the probabilities of missed detection and false alarm?

Constraints:

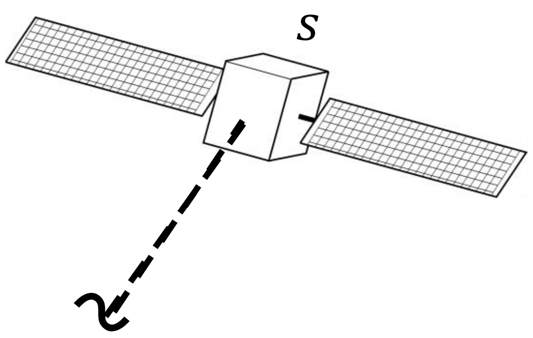
- Instantaneous
- Commercial off the shelve, (low cost) receivers
- Easy implementation on (military) platform systems

Assumption:

- All satellites used for the position solution are either genuine or counterfeit

Contents

Theoretical observation model



Carrier phase observation model:

$$\phi_r^s \lambda = \rho_r^s + c(dt_r - dt^s) + \lambda(d\phi_r - d\phi^s + N_r^s) + A_r^s + \epsilon_r^s$$

Single differenced carrier phase observation model:

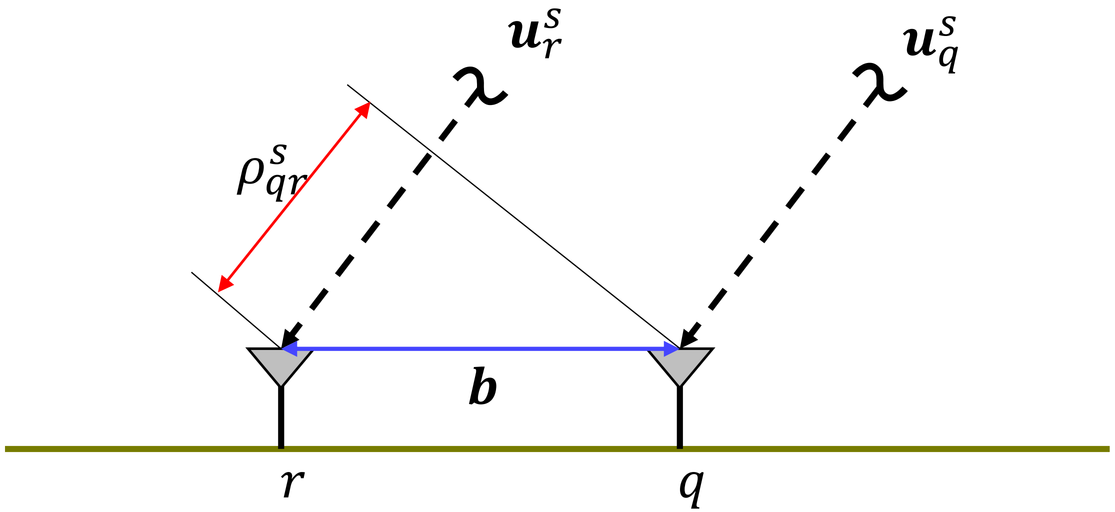
$$\lambda \phi_{qr}^s = \rho_{qr}^s + c\ dt_{qr} + \lambda\left(d\phi_{qr} + N_{qr}^s\right) + \epsilon_{qr}^s$$

With the line of sight vector:

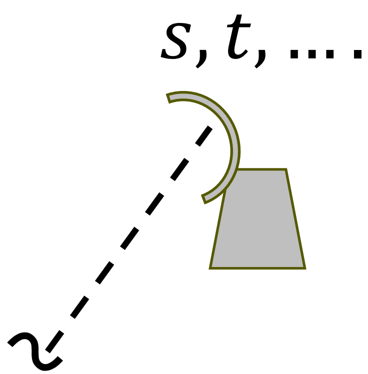
$$\boldsymbol{u}_r^s \approx \boldsymbol{u}_q^s \approx \boldsymbol{u}_0^s$$

We can write:

$$\rho_{qr}^s = (\boldsymbol{u}_0^s)^T \cdot \boldsymbol{b}$$



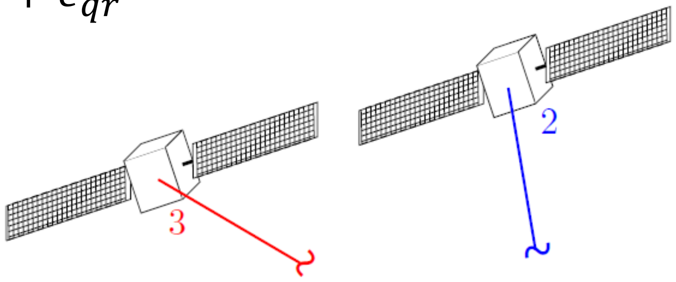
Theoretical observation model



Carrier phase observation model (normal conditions):

$$\lambda\phi_{qr}^{s} = (\boldsymbol{u}_0^{s})^T \cdot \boldsymbol{b} + c\, dt_{qr} + \lambda\big(d\phi_{qr} + N_{qr}^{s}\big) + \epsilon_{qr}^{s}$$

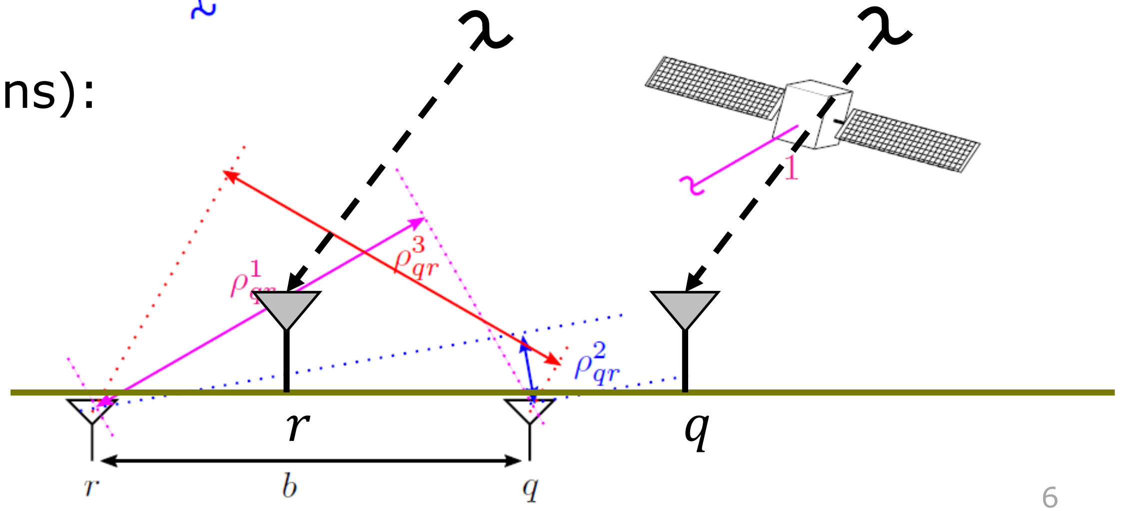
Different for each satellite



Carrier phase observation model (spoofed conditions):

$$\lambda\phi_{qr}^{s} = \left(\boldsymbol{u}_0^{f}\right)^T \cdot \boldsymbol{b} + c\, dt_{qr} + \lambda\big(d\phi_{qr} + N_{qr}^{s,f}\big) + \epsilon_{qr}^{s,f}$$

Equal for all satellites



Theoretical observation model

SD genuine: $\lambda\phi_{qr}^{s} = (\boldsymbol{u}_0^s)^T \cdot \boldsymbol{b} + c\ dt_{qr} + \lambda\left(d\phi_{qr} + N_{qr}^{s}\right) + \epsilon_{qr}^{s}$

SD spoofed: $\lambda\phi_{qr}^{s} = \left(\boldsymbol{u}_0^f\right)^T \cdot \boldsymbol{b} + c\ dt_{qr} + \lambda\left(d\phi_{qr} + N_{qr}^{s,f}\right) + \epsilon_{qr}^{s,f}$

Constructing Double Differenced (DD) observations results in:

DD genuine: $\lambda\phi_{qr}^{st} = (\boldsymbol{u}_0^{st})^T \cdot \boldsymbol{b} + \lambda\left(N_{qr}^{st}\right) + \epsilon_{qr}^{st}$

DD spoofed: $\lambda\phi_{qr}^{st} = \lambda\left(N_{qr}^{st,f}\right) + \epsilon_{qr}^{st,f}$

Introducing fractional phase observations: $\tilde{\phi}_{qr}^{st} = \phi_{qr}^{st} - round\left[\phi_{qr}^{st}\right]$

DD genuine: $\tilde{\phi}_{qr}^{st} = B_{qr}^{st} + e_{qr}^{st}$

DD spoofed: $\tilde{\phi}_{qr}^{st} = 0 + e_{qr}^{st,f}$

Hypothesis testing model

Assumption: $\tilde{\phi}_{qr}^{st} \sim N(B_{qr}^{st}, \sigma_{DD}^2)$

Lets define:

$$\Phi = \left[\tilde{\phi}_{12}^{12}, \tilde{\phi}_{12}^{13}, \dots \dots \tilde{\phi}_{12}^{1m}\right]^T$$

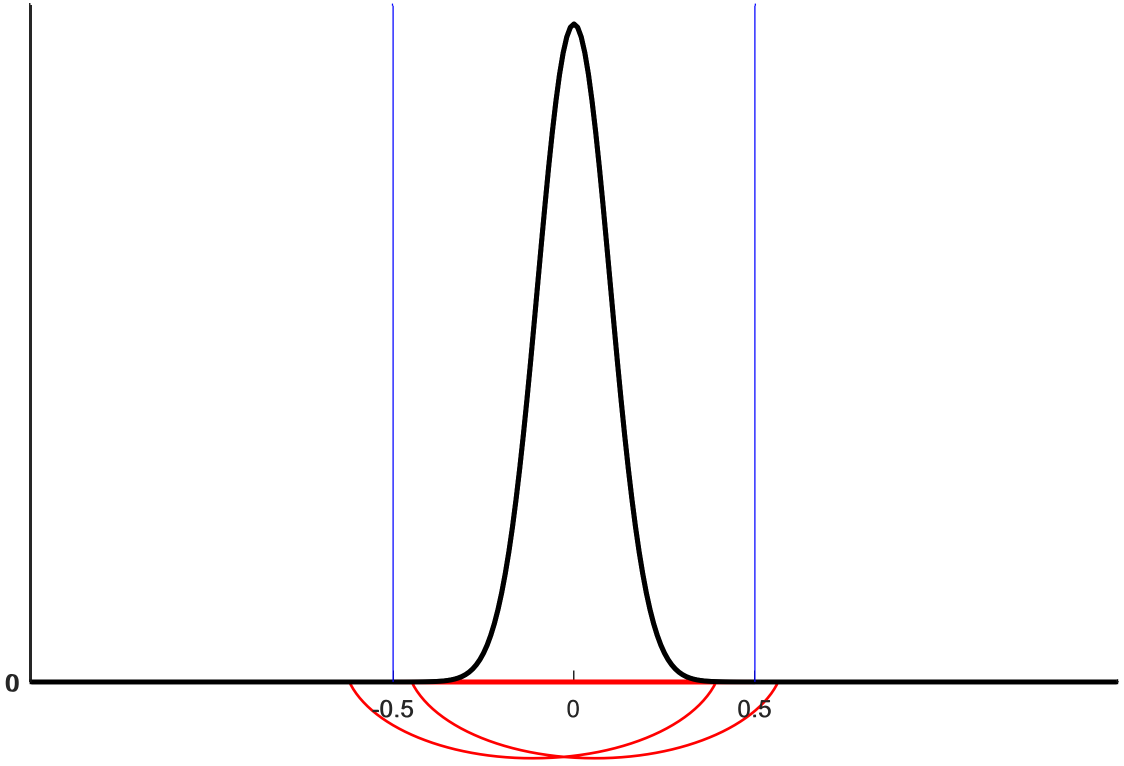
Valid if $|\boldsymbol{b}| > \lambda$, verified using simulations

Stochastic hypothesis

H_0: $\Phi \sim U\left(-\frac{1}{2}, \frac{1}{2}\right)$

H_A: $\Phi \sim N(0, \sigma_{DD}^2)$

Assumption $\sigma_{DD} \ll \lambda$



Test statistic

Applying the Simple Likelihood Ratio test leads to the following test statistic:

$$T_s = \Phi^T Q_\phi^{-1} \Phi$$

Reject H_0 if $T_s < k_\alpha$

Test statistic for normally distributed observations (H_A) =>m-dimensional central Chi-Squared distribution

However, the H_0 results in the sum of squared uniformly distributed observations => no closed form of the distribution, very complex situation

Monte-Carlo simulation!!

Probability of false alarm and missed detection

Type I error:

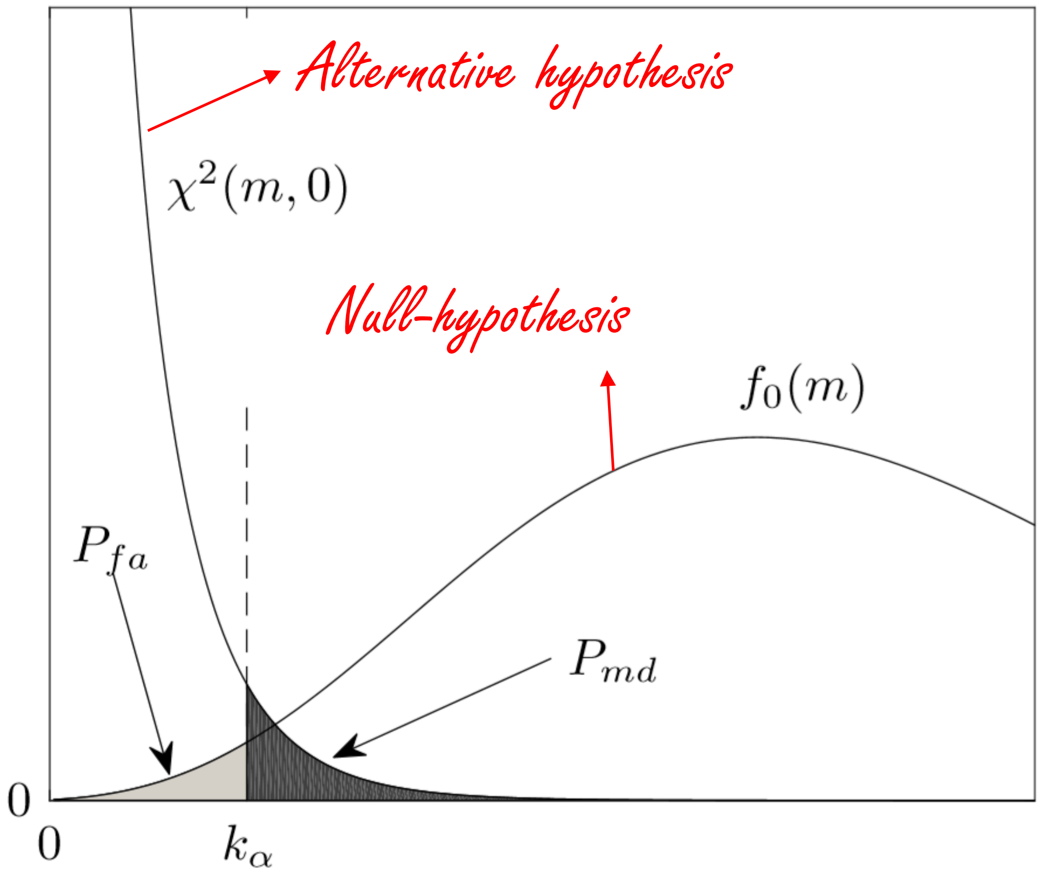
- Rejection of H_0 when in fact H_0 is true.
- false alarm

Continuity & availability

Type II error:

- Acceptance of H_0 when in fact H_0 is false.
- missed detection

Integrity



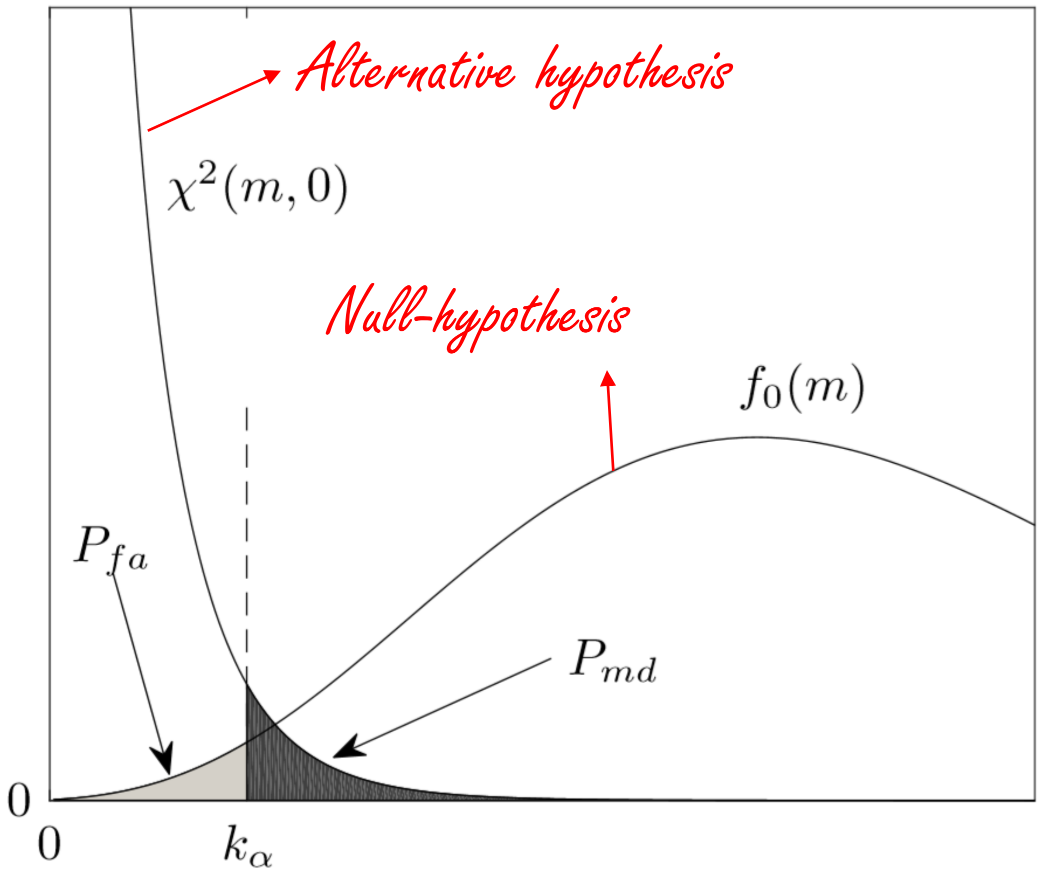
Probability of false alarm and missed detection

k_α directly influences the P_{md} and P_{fa}.

So, how to determine k_α?

Two options:

- Determine k_α based on a fixed P_{md} then determine P_{fa}
- Determine k_α based on a fixed P_{fa} then determine P_{md}



Monte-Carlo simulation

- Estimation of the false alarm rate
  - Calculate test statistic for each combination of P_{md}, σ_f and m
  - 10^9 random uniformly distributed samples per combination
  - Calculate the test statistic T_s
  - Determine for how many samples $T_s < k_\alpha$ (false alarm)

	$\mathbf{P_{md}} = 0.001$					
m	$\sigma_f =$ 0.01	$\sigma_f =$ 0.02	$\sigma_f =$ 0.03	$\sigma_f =$ 0.04	$\sigma_f =$ 0.05	$\sigma_f =$ 0.10
3	2.8e-04	2.2e-03	7.4e-03	1.8e-02	3.4e-02	2.7e-01
4	1.7e-05	2.7e-04	1.4e-03	4.3e-03	1.1e-02	1.7e-01
5	9.6e-07	3.2e-05	2.4e-04	1.0e-03	3.1e-03	1.0e-01
6	5.1e-08	3.8e-06	4.2e-05	2.4e-04	9.1e-04	5.9e-02
7	4.0e-09	4.2e-07	7.3e-06	5.5e-05	2.6e-04	3.4e-02
8	<1.0e-9	5.6e-08	1.2e-06	1.2e-05	7.4e-05	1.9e-02
9	<1.0e-9	6.0e-09	2.0e-07	2.8e-06	2.1e-05	1.1e-02
10	<1.0e-9	<1.0e-9	4.5e-08	6.2e-07	5.7e-06	5.8e-03
11	<1.0e-9	1.0e-09	4.0e-09	1.1e-07	1.5e-06	3.1e-03
12	<1.0e-9	<1.0e-9	1.0e-09	3.6e-08	4.0e-07	1.7e-03
13	<1.0e-9	<1.0e-9	<1.0e-9	7.0e-09	1.0e-07	9.1e-04
14	<1.0e-9	<1.0e-9	<1.0e-9	<1.0e-9	3.4e-08	4.8e-04
15	<1.0e-9	<1.0e-9	<1.0e-9	<1.0e-9	8.0e-09	2.5e-04

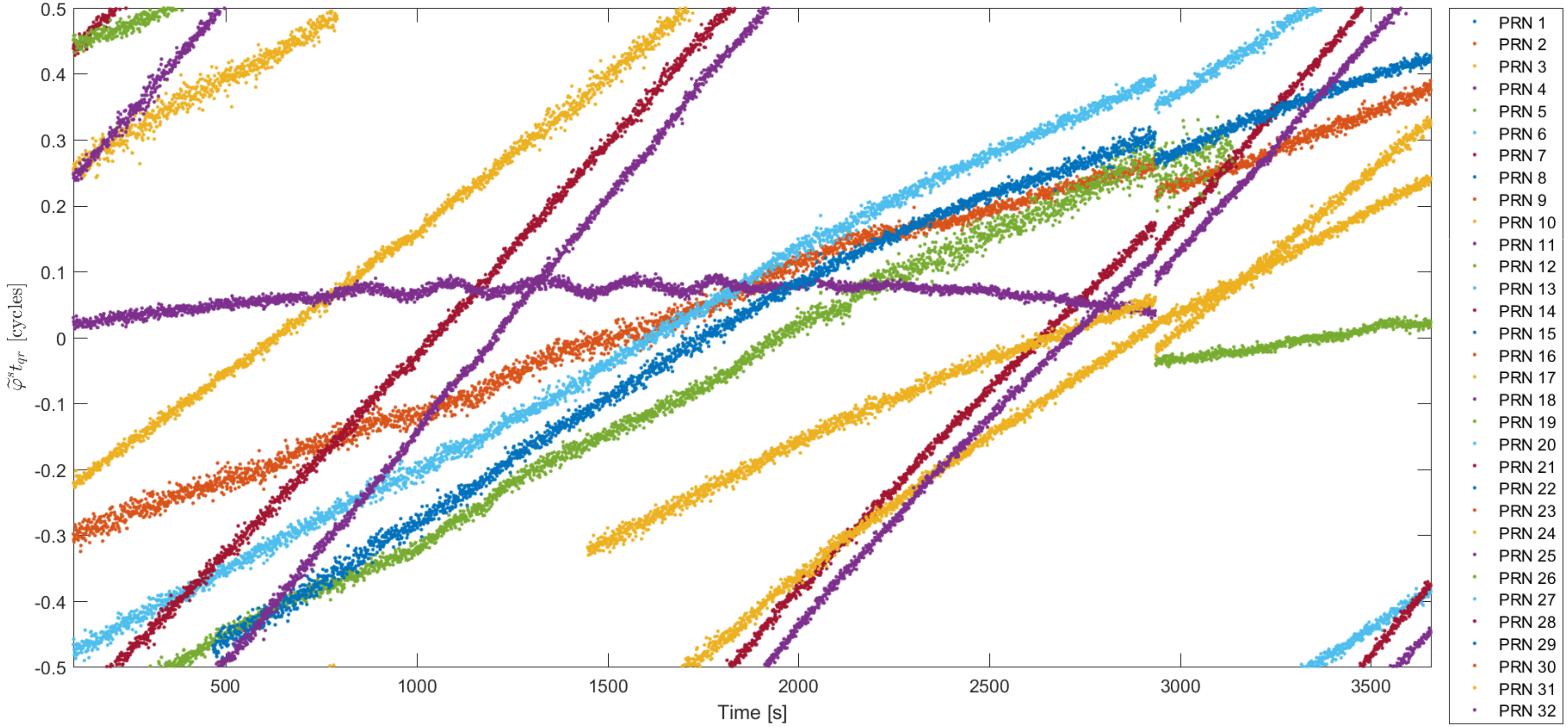
0

Experiment

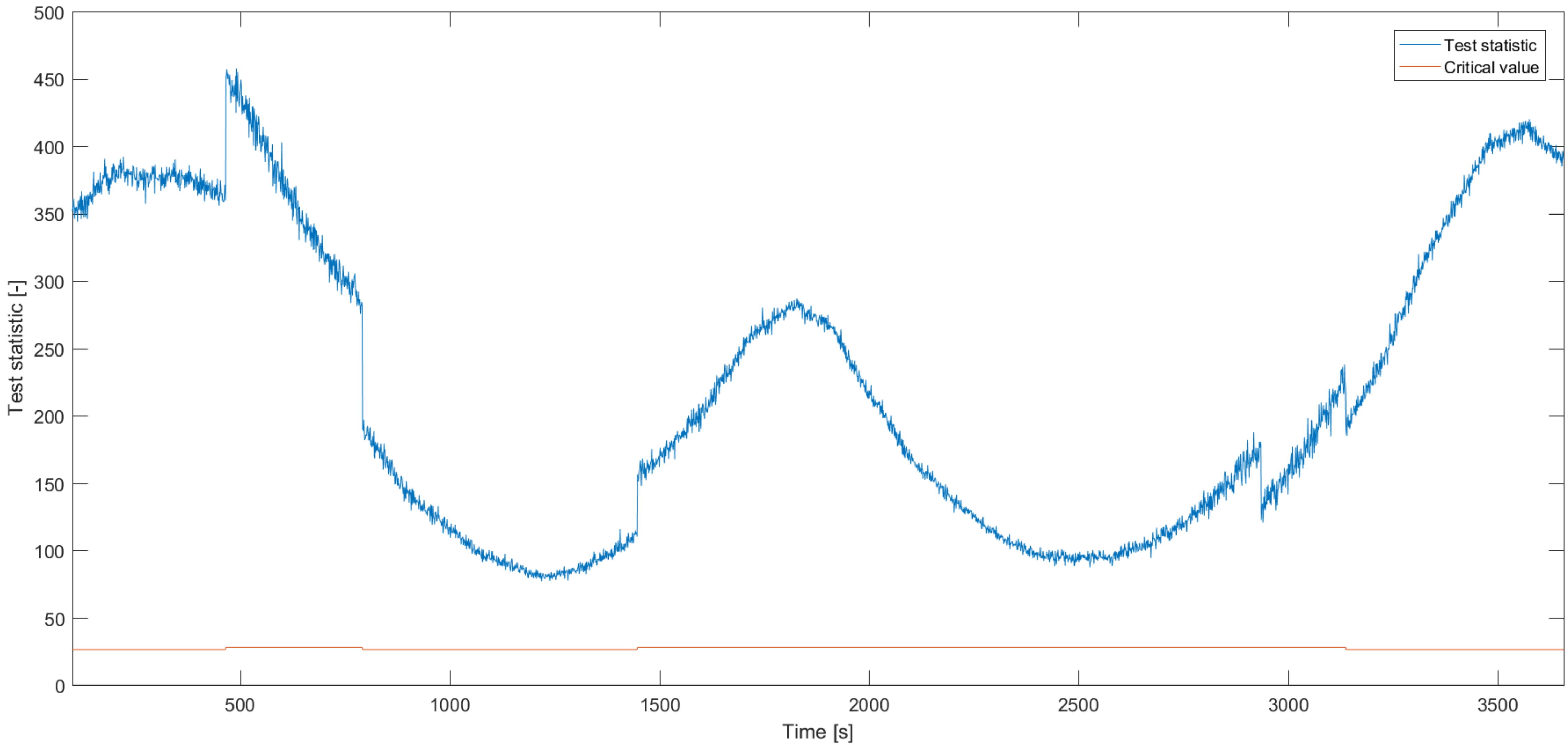

Source: Damen

TEST LOCATIONS

Experimental results – Sea dyke



Results: Dyke, Test statistic



Observations based on more genuine observations

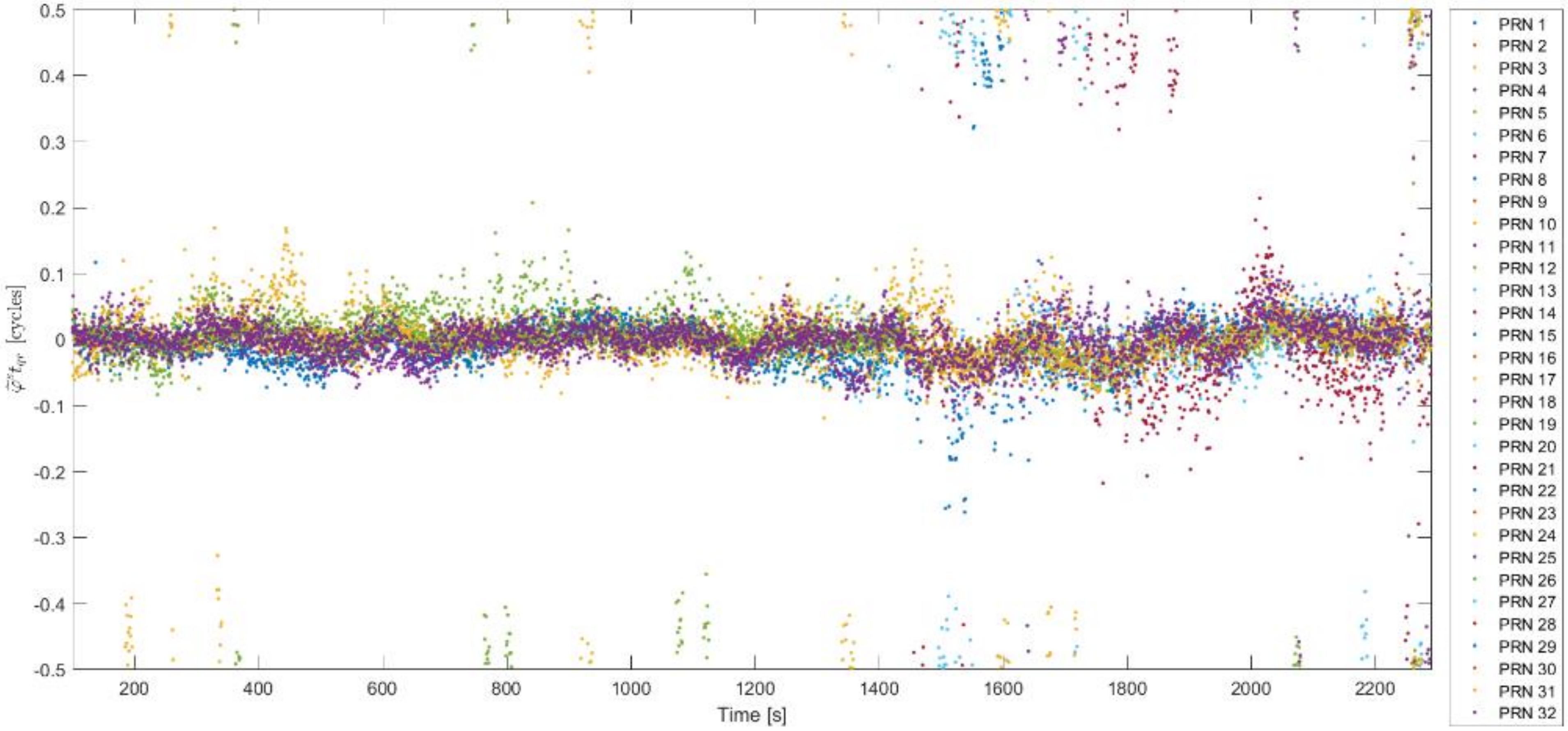
- In total 216 minutes of genuine observations @ 1Hz (~13000 epochs)
- For testing it is assume that $\sigma_f = 0.10$ cycles
- On average 9 satellites visible (elevation cutoff @ 5 deg)

Worst case scenario

- $P_{md} = 0.001$
  - 94 alerts ($\mathrm{P_{fa}} = 7.2 \times 10^{-3}$)
- $P_{md} = 0.01$
  - 60 alerts ($\mathrm{P_{fa}} = 5.2 \times 10^{-3}$)
- $P_{md} = 0.1$
  - 9 alerts ($\mathrm{P_{fa}} = 6.9 \times 10^{-4}$)

$\mathrm{P_{md}} = 0.1$						
m	$\sigma_f =$ 0.01	$\sigma_f =$ 0.02	$\sigma_f =$ 0.03	$\sigma_f =$ 0.04	$\sigma_f =$ 0.05	σ_f 0.10
3	6.5e-05	5.2e-04	1.8e-03	4.2e-03	8.2e-03	6.5e-02
4	3.0e-06	4.8e-05	2.4e-04	7.6e-04	1.9e-03	3.0e-02
5	1.5e-07	4.5e-06	3.3e-05	1.4e-04	4.3e-04	1.4e-02
6	1.1e-08	3.9e-07	4.6e-06	2.6e-05	9.7e-05	6.2e-03
7	<1.0e-9	3.5e-08	6.4e-07	4.6e-06	2.2e-05	2.8e-03
8	<1.0e-9	3.0e-09	1.0e-07	8.6e-07	5.0e-06	1.3e-03
9	<1.0e-9	1.0e-09	1.2e-08	1.5e-07	1.2e-06	5.9e-04
10	<1.0e-9	<1.0e-9	2.0e-09	3.4e-08	2.6e-07	2.7e-04
11	<1.0e-9	<1.0e-9	<1.0e-9	1.1e-08	5.2e-08	1.2e-04
12	<1.0e-9	<1.0e-9	<1.0e-9	5.0e-09	1.6e-08	5.5e-05
13	<1.0e-9	<1.0e-9	<1.0e-9	<1.0e-9	5.0e-09	2.4e-05
14	<1.0e-9	<1.0e-9	<1.0e-9	<1.0e-9	<1.0e-9	1.1e-05
15	<1.0e-9	<1.0e-9	<1.0e-9	<1.0e-9	<1.0e-9	4.9e-06

Experimental results – Patrol vessel



Outlier detection and removal

- Z-score
  - Standard deviation required

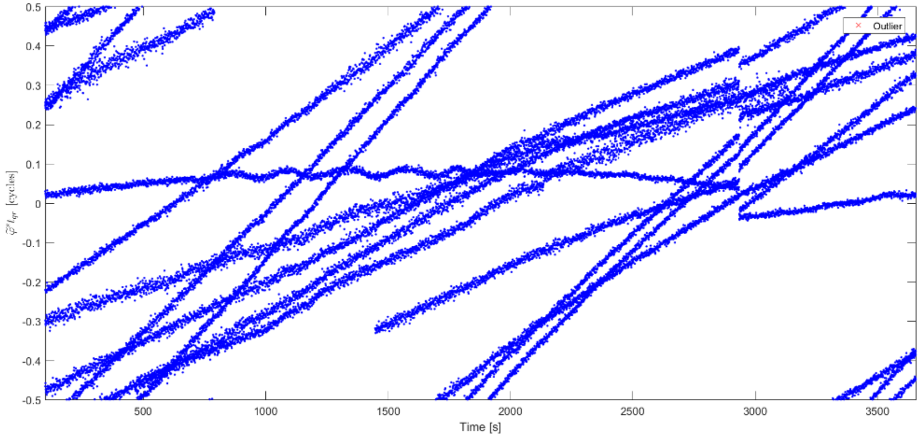
- More robust: Modified Z-score

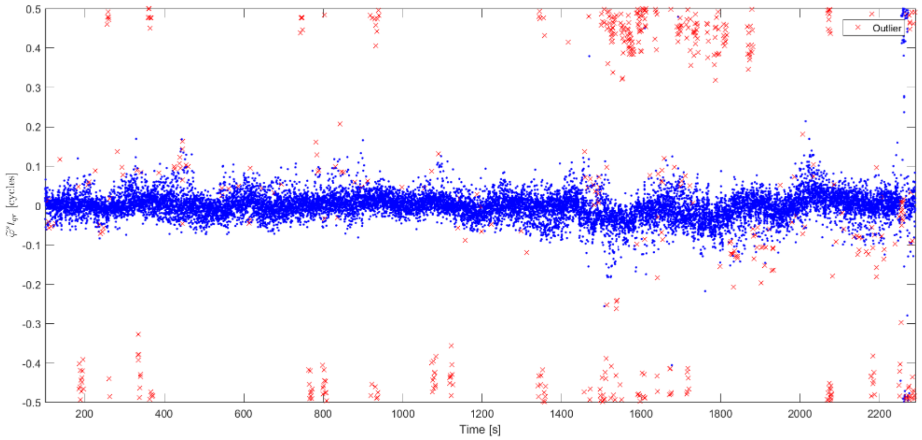
$$M_{qr}^{ts} = \frac{\tilde{\phi}_{qr}^{ts} - median(\tilde{\Phi})}{MAD}$$

With

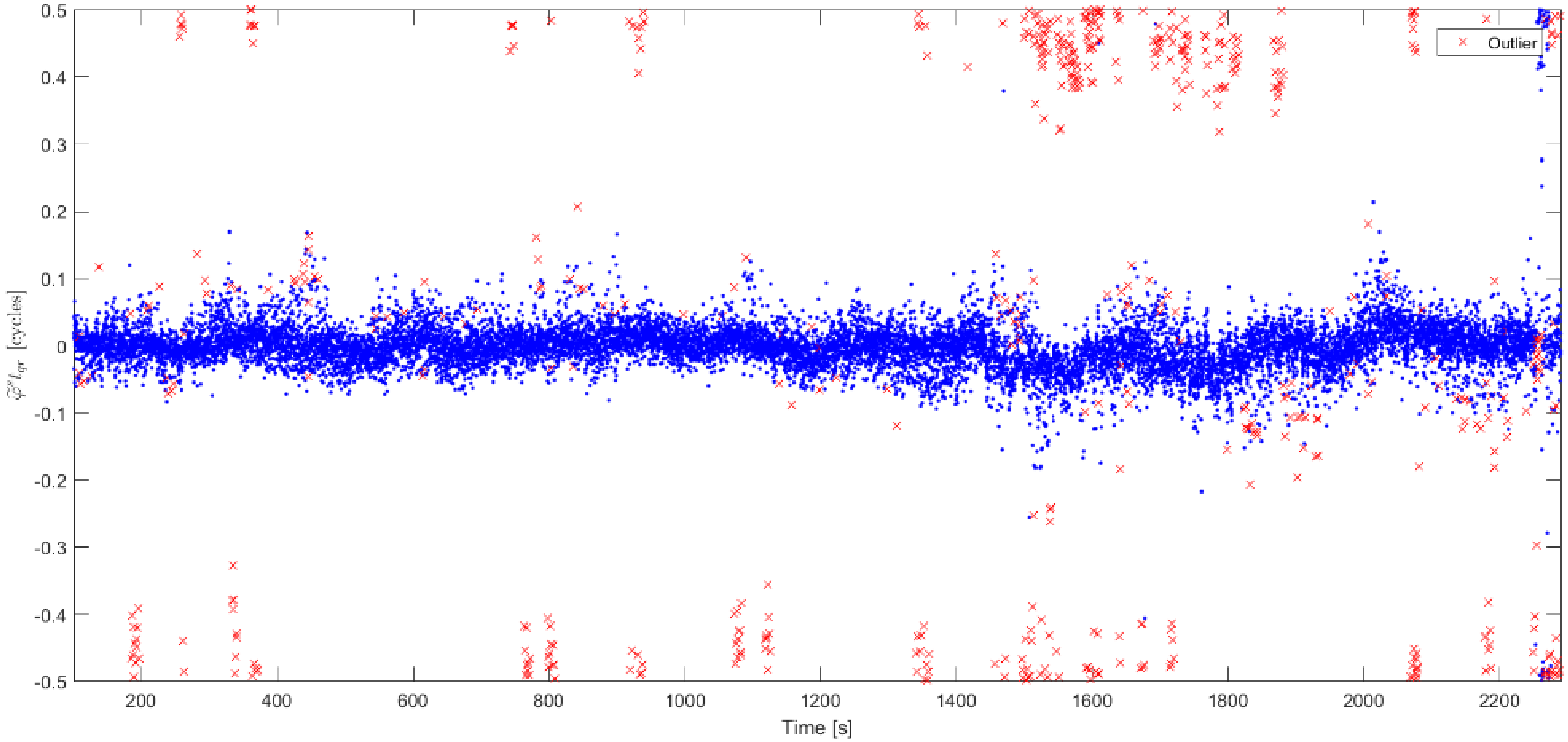
$$MAD = 1.483\, median\left|\phi_{qr}^{ts} - median(\tilde{\Phi})\right|$$

Remove observation if M_{qr}^{ts} > threshold

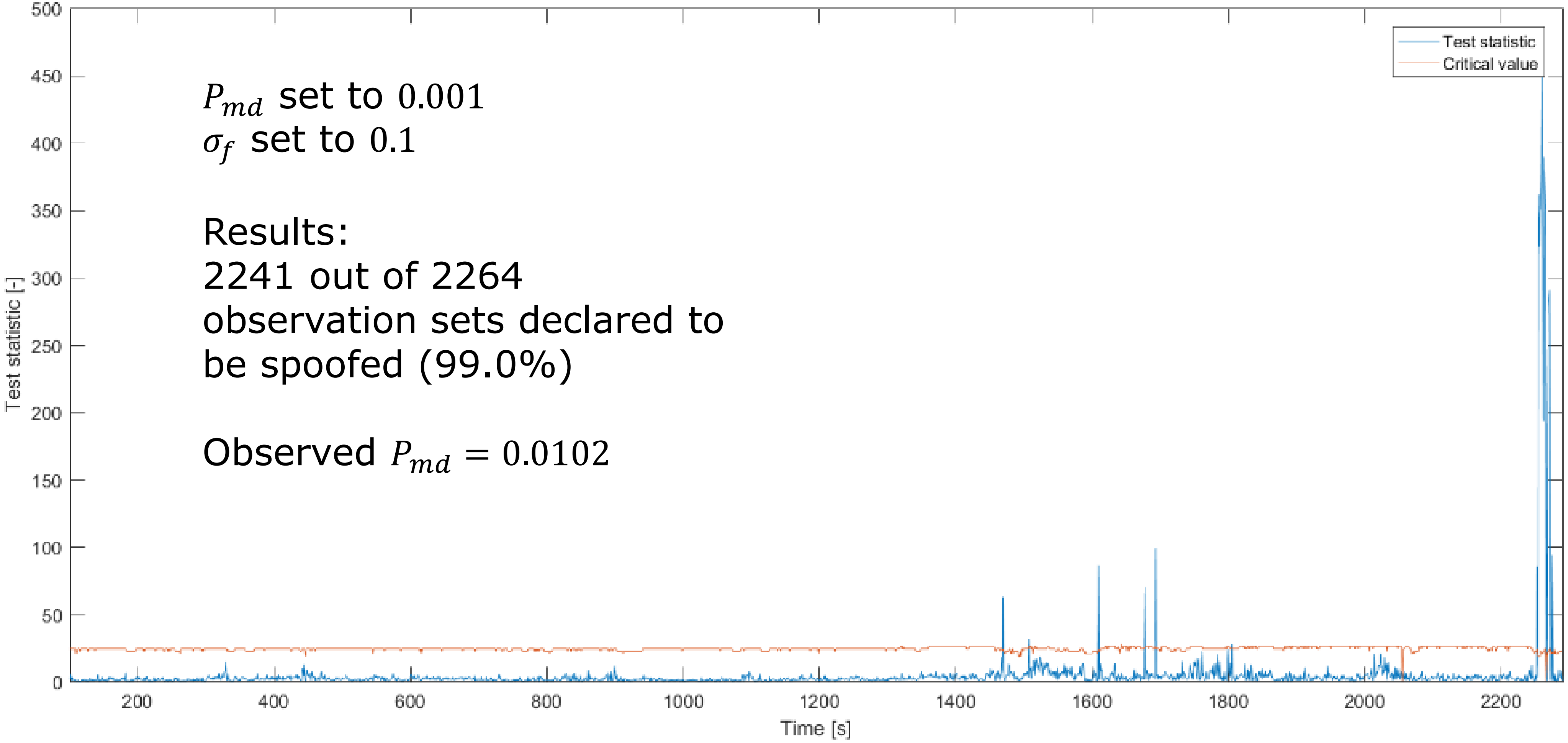




Experimental results – Patrol vessel



Experimental results – Patrol vessel

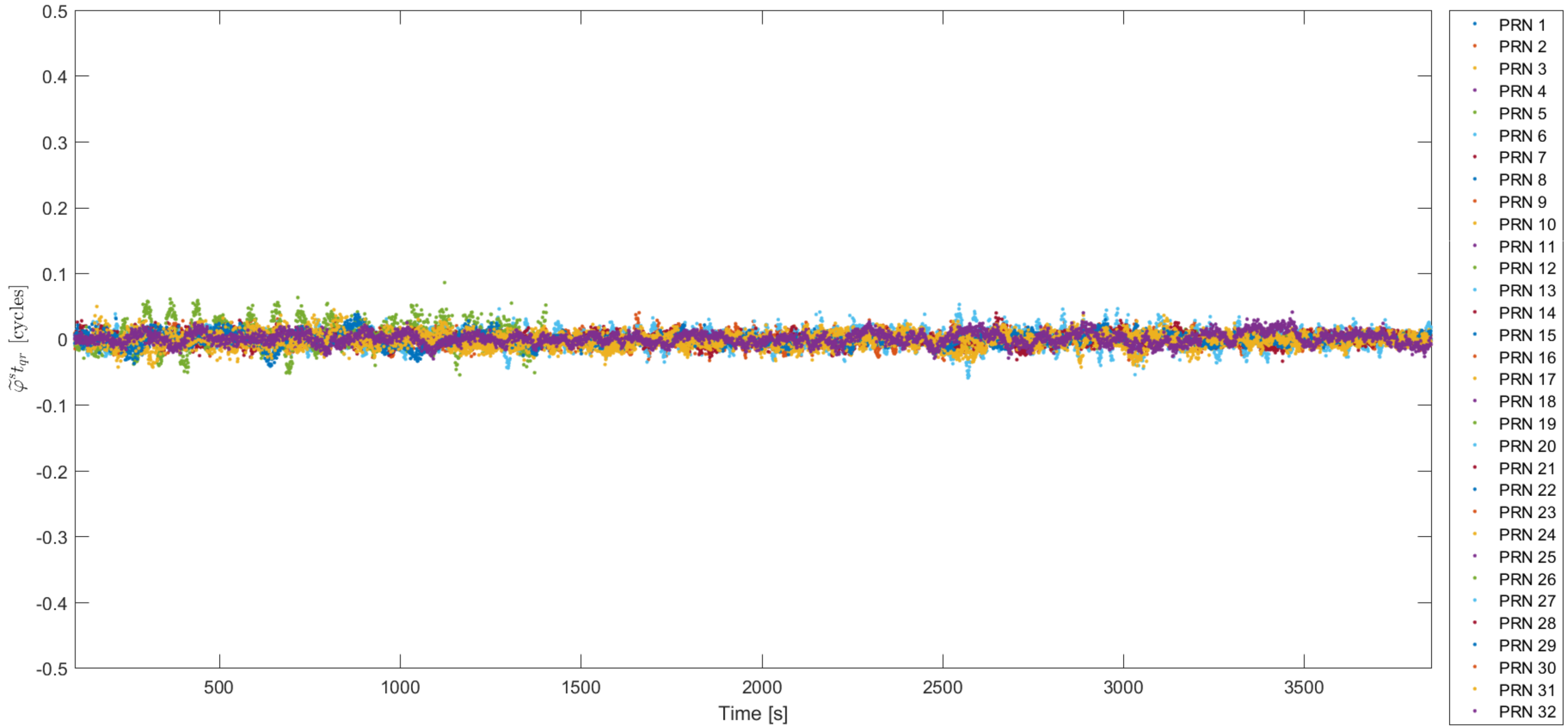


P_{md} set to 0.001
σ_f set to 0.1

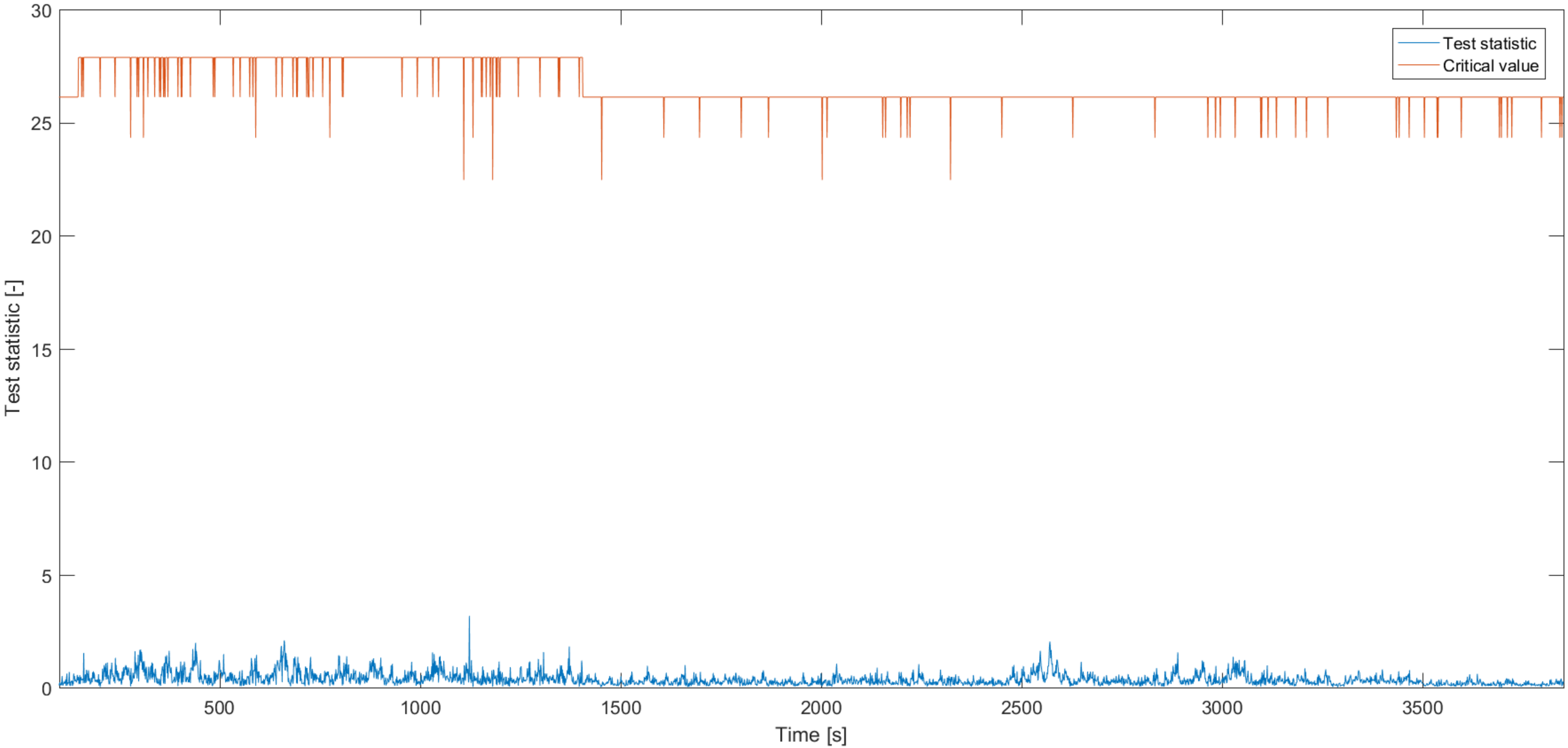
Results:
2241 out of 2264 observation sets declared to be spoofed (99.0%)

Observed $P_{md} = 0.0102$

Experimental results – Schiphol



Results: Hangar, Test statistic



Conclusions

- Measurements confirm theory
- Method seems to be a very simple but effective spoofing detection method
- Reasonable probabilities of missed detection and false alarm possible

Future work

- Validate method with more data
- Expand method from static to dynamic
- Determine realistic noise levels for spoofed observations

Thank you for your attention!