GATEMAN Workshop
8th SESAR Innovation Days

4. Spoofing Detection and Signal DF Algorithms

Gianluca Falco, Emanuela Falletti
[ISMB]

Salzburg 3rd December 2018

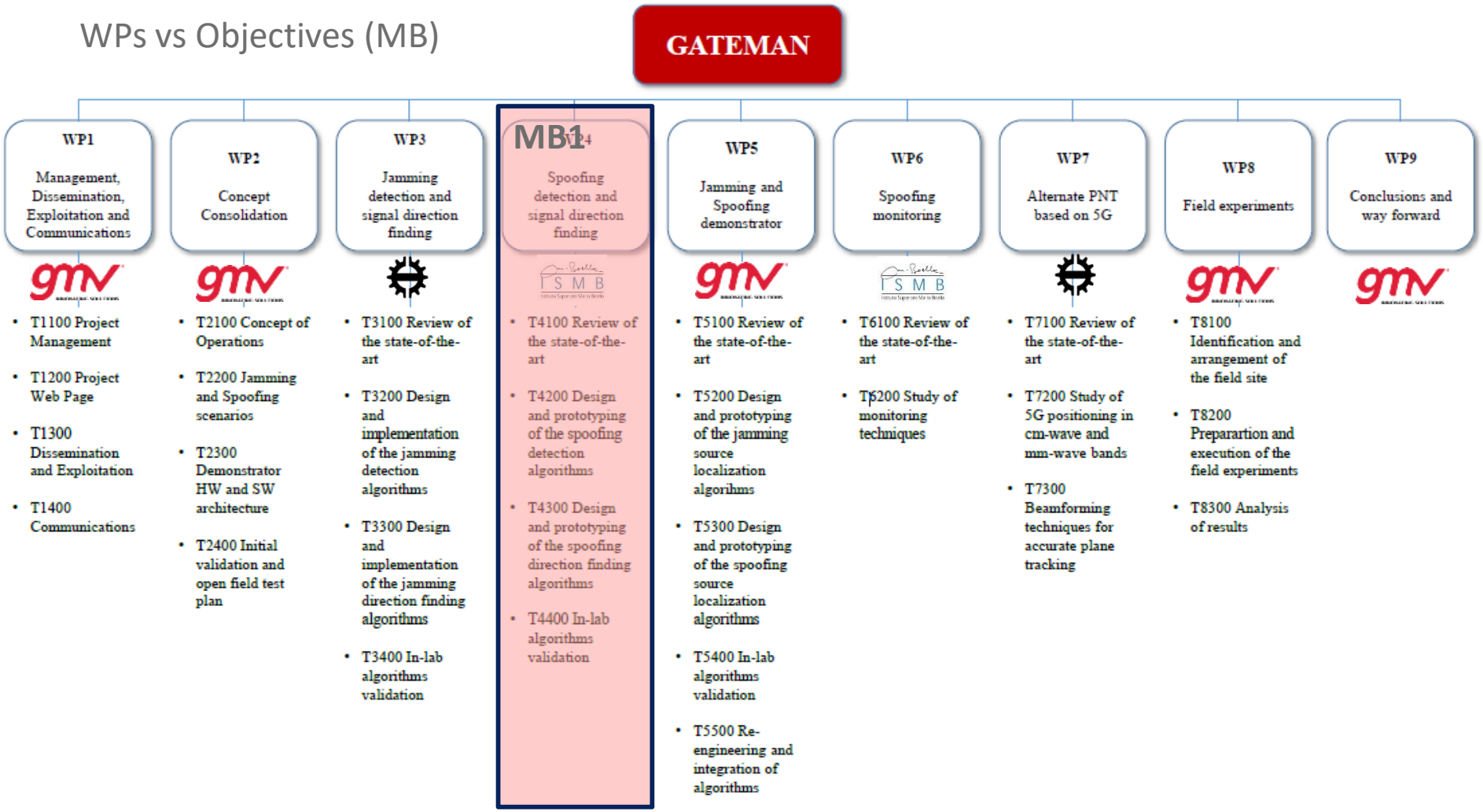
SESAR JOINT UNDERTAKING

Founding Members

EUROPEAN UNION EUROCONTROL

Context in GATEMAN

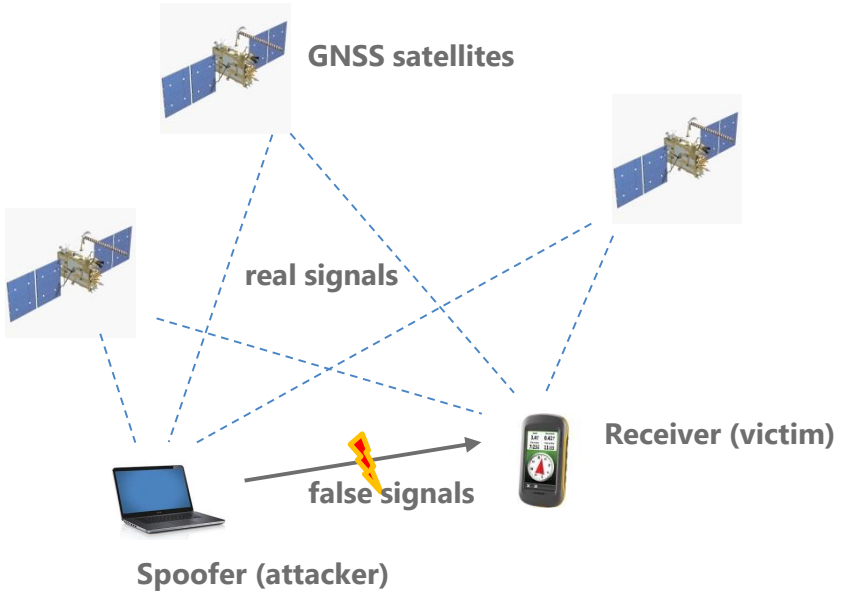
WPs vs Objectives (MB)



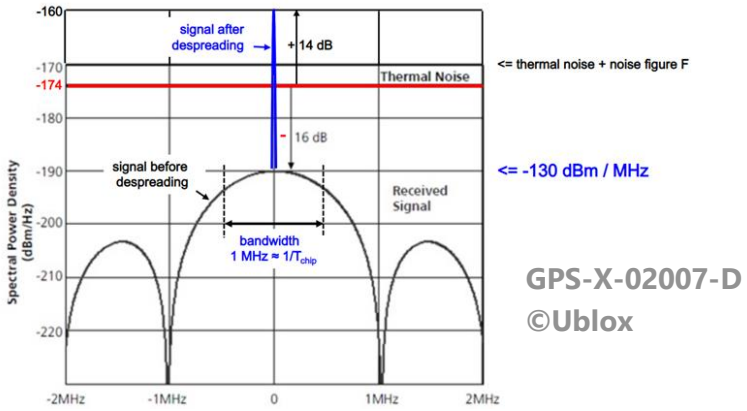
Outline

- **GNSS Spoofing: Real Events and Main Concepts**
- Spoofing Detection – Angle of Arrival Defence
  - The Sum-of-Squares Method
  - The dispersion of the double differences (D^3) Method
- Spoofing Direction of Arrival (DoA) Estimation
  - A “Precise and Fast” Approach
  - Some tests in the lab & Results
- Conclusions

RF spoofing



A **RF spoofing** attack deceives the target receiver with a counterfeit ensemble of the GNSS signal



GPS-X-02007-D
©Ublox

- More malicious than jamming: the false signals take control of the target receiver and the victim is fooled without any notice;
- Attacks can be very effective depending on the quality of the generated signal

Structured interference

Some famous demos

LORENZO FRANCESCHI-BICCHIERAI SECURITY 07.06.12 06:30 AM

DRONE HIJACKING? THAT'S JUST THE START OF GPS TROUBLES

The University of Texas Radionavigation Laboratory drone, an Adaptive Flight Hornet Mini.

PHOTO: COURTESY TODD HUMPHREYS

NEW ATLAS

LIFESTYLE SCIENCE TECHNOLOGY TRANSPORT SE

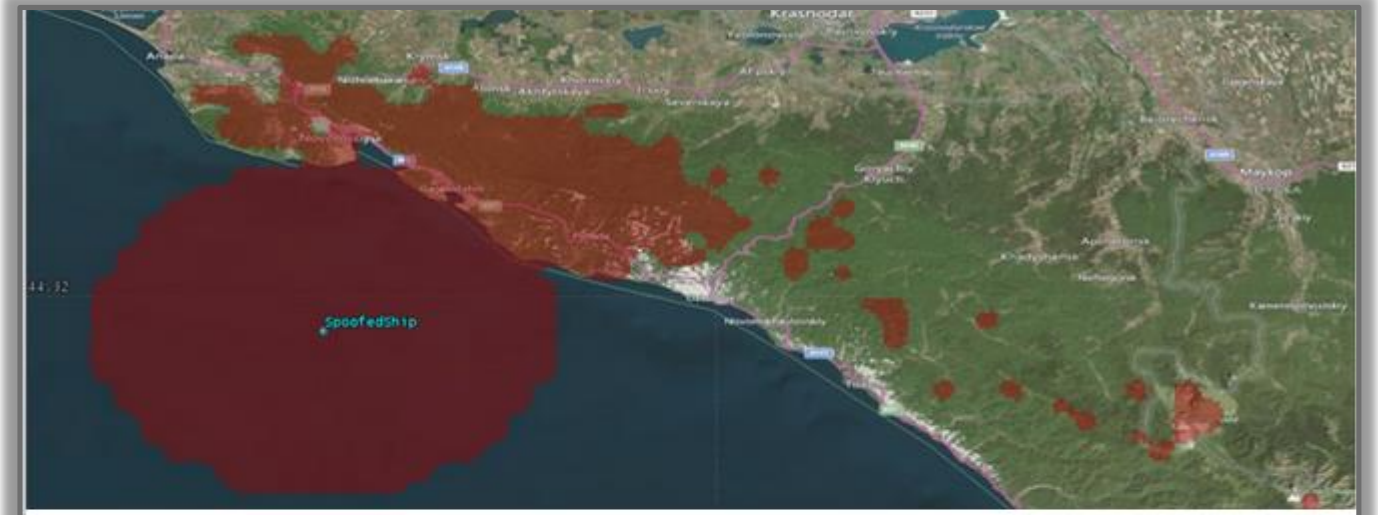
MARINE

University of Texas team takes control of a yacht by spoofing its GPS

Brian Dodson | August 11th, 2013

The 213-foot White Rose is the US$80M megayacht whose GPS navigational system was spoofed by about $2,000-$3,000 worth of equipment (Photo: U of Texas at Austin)

A real spoofing attack (2017)



Spoofing in the Black Sea: What really happened?

October 11, 2017 - By Michael Jones

Est. reading time: 8:30

Facebook Twitter Google LinkedIn

We've heard a lot in the news recently about GPS spoofing, mostly centr
of ship spoofing in the Black Sea. Between June 22-24, a number of ship
Sea reported anomalies with their GPS-derived position, and found them
apparently located at an airport.

What happened is open to educated conjecture. In this column, I'll briefl

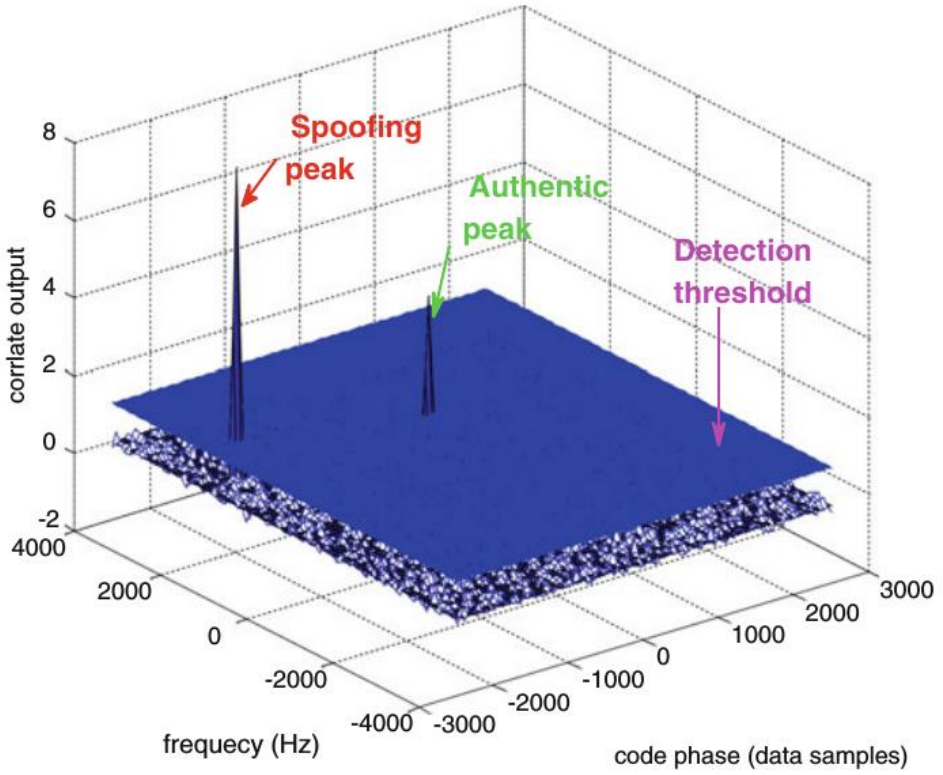
Between June 22-24, **more than 20 vessels in the Black Sea** reported anomalies with their GPS position, and **found themselves** apparently **located at an airport.**

available @: http://gpsworld.com/spoofing-in-the-black-sea-what-really-happened/?utm_source=gps_defense&utm_medium=email&utm_campaign=gps_defense_10112017&eid=397565451&bid=1892311

Spoofing basics

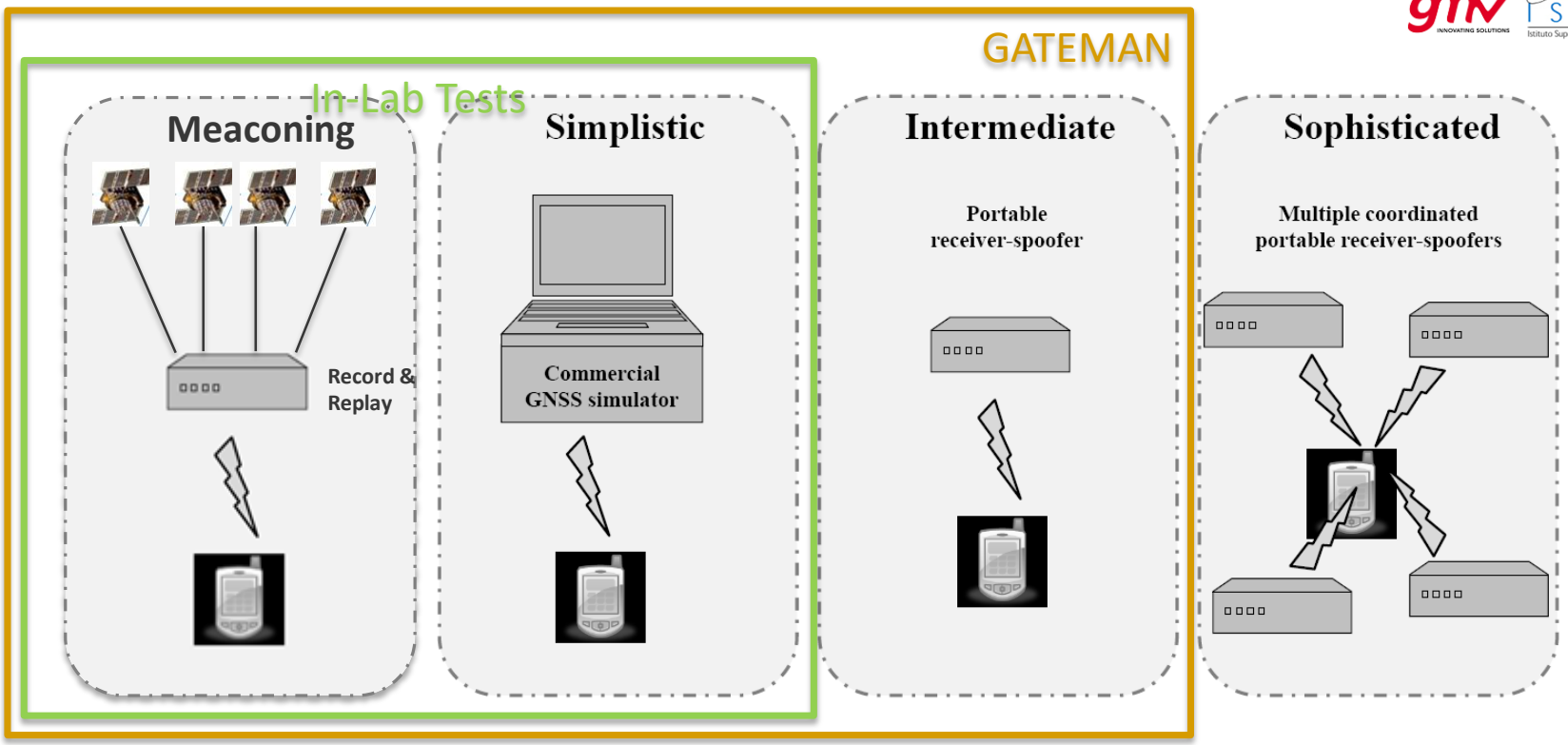
A receiver searches for a satellite over a two-dimensional surface (Doppler frequencies and code offsets) to find a **correlation peak**

- A **spoofer** fools the victim receiver, trying to recreate a secondary peak.
- The receiver will begin to track the spoofed signal and **the spoofer can begin to manipulate reality** by slowly modifying the properties of the signal.



[1] M. Jones, "Spoofing in the Black Sea: What really happened?", GPS World, October 2017

Classification of Spoofing Attacks

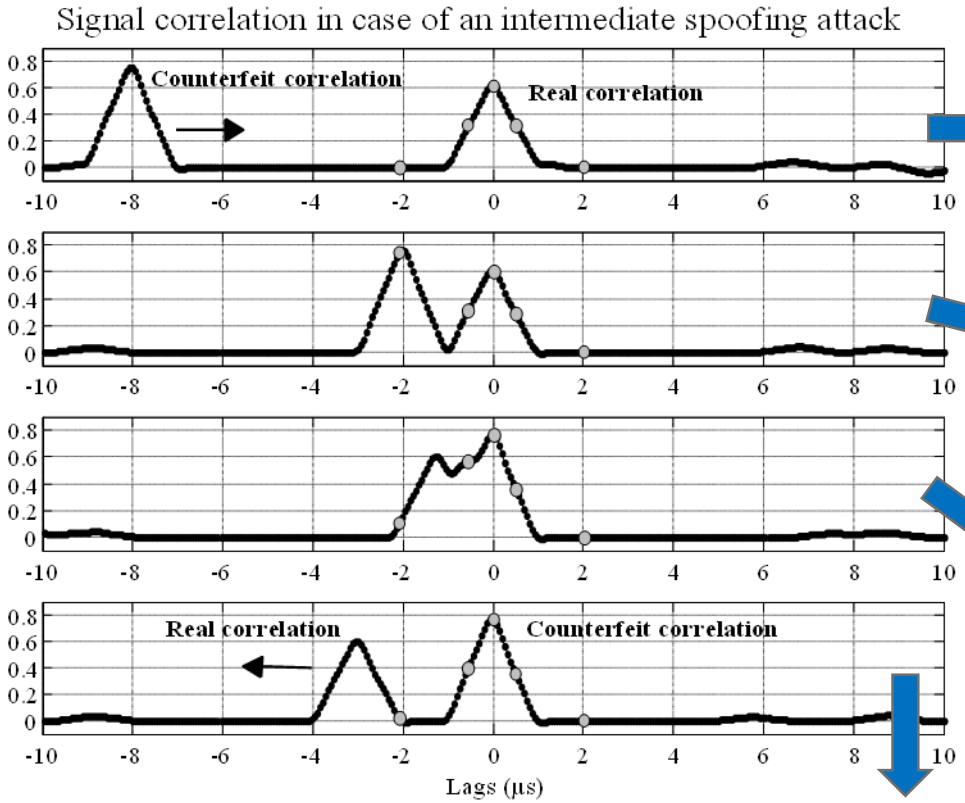


[2] Humphreys T., Ledvina B. M., Psiaki M. L., O'Hanlon B. W., Kintner P. M., "Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer," *in Proc. of the 21st International Technical Meeting of the Satellite Division of The Institute of Navigation* (ION GNSS 2008), Savannah, GA, September 2008, pp. 2314-2325.

[3] Ledvina B. M., Bencze W. J., Galusha B., Miller I., "An In-Line Anti-Spoofing Device for Legacy Civil GPS Receivers," *in Proc. of the 2010 International Technical Meeting of The Institute of Navigation*, San Diego, CA, January 2010, pp. 698-712.

[4] D. Margaria, B. Motella, M. Anghileri, J. J. Floch, I. Fernandez-Hernandez and M. Paonni, "Signal Structure-Based Authentication for Civil GNSSs: Recent Solutions and Perspectives,"in IEEE Signal Processing Magazine, vol. 34, no. 5, pp. 27-37, Sept. 2017. doi: 10.1109/MSP.2017.2715898

E.g. The Effect on the Correlation Peak



Initial phase The spoofing signal is active, but still 'far' from the true correlation peak

Approaching phase The counterfeit peak approaches the true one.

Overlapping phase The counterfeit signal distorts the true correlation peak and forces a signal lift-off (if the signal power is higher than the real one). The distortion on the correlation function induced by the spoofed signal can be detected by SQM algorithms

Dropping phase. The spoofing signal power is sufficiently high to force the receiver to stay locked on the counterfeit signal, that is delayed in order to introduce an error.

List of Spoofing Countermeasures: USER LEVEL

Positioning	**Receiver Autonomous Integrity Monitoring (RAIM)**	Integrity Check among Different Pseudorange Measurements
	Consistency Cross Check with Other Navigation Systems	Cross check with IMU solutions, Cross check with cellular and Wi-Fi positioning solutions
Data Bits	**Time of Arrival (TOA) Methods**	Monitoring the bit transition boundaries
	Navigation Message Analysis	Consistency check among satellites navigation messages
Signal Processing	**Correlation Peak Monitoring**	Signal Quality Monitoring (SQM), Monitoring the distribution of correlation peak.
	Spatial Discrimination of Spoofing Signals	Antenna Array Processing, Synthetic Antenna Arrays
	Power Based Methods	C/N0 Monitoring, Absolute Power Monitoring, L1/L2 Power level Comparison, …

[5] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "GPS spoofer countermeasure effectiveness based on signal strength, noise power and C/N0 observables," International Journal of Satellite Communications and Networking, vol. 30, no. 4, pp. 181–191, 2012.

Outline

- GNSS Spoofing: Real Events and Main Concepts
- **Spoofing Detection – Angle of Arrival Defence**
  - **The Sum-of-Squares Method**
  - The dispersion of the double differences (D^3) Method
- Spoofing Direction of Arrival (DoA) Estimation
  - A “Precise and Fast” Approach
  - Some tests in the lab & Results
- Conclusions

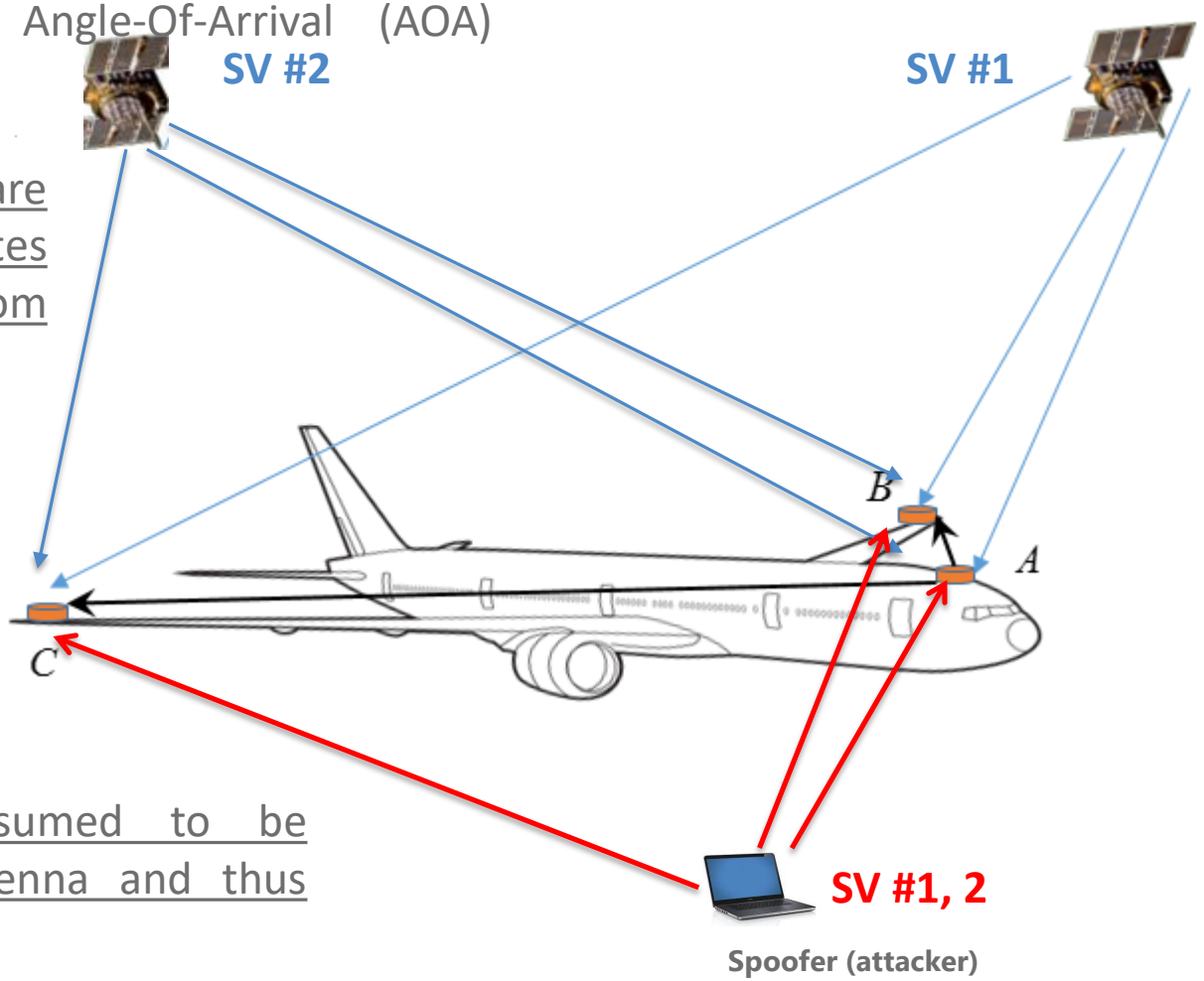
Angle of Arrival Defence

One of the most effective approaches for spoofing detection is the so-called Angle-Of-Arrival (AOA) defence.

Genuine GNSS signals are transmitted by different satellites and arrive at the receiver from different directions.

The AOA of the signals received depends on the satellite and receiver relative position and can be estimated using an antenna array.

Counterfeit signals are assumed to be broadcast from a single antenna and thus share a common AOA



[6] D. Borio and C. Gioia. "A dual-antenna spoofing detection system using GNSS commercial receivers", in Proc of ION GNSS+ 2015, Tampa, FL, USA, Sep. 2015, pp.1–6

Spoofing Detection – AOA methods

A multi-antenna system can be used to verify if all the signals received share the same AOA

Some approaches for Spoofing detection based on AOA are available in the scientific literature [7], [8], **but** they are:

1. **Complex** (they require to work with carrier phase differences);
2. **Integer ambiguities needs to be estimated after forming Single Differences;**
3. **The systems developed require dedicated hardware.**

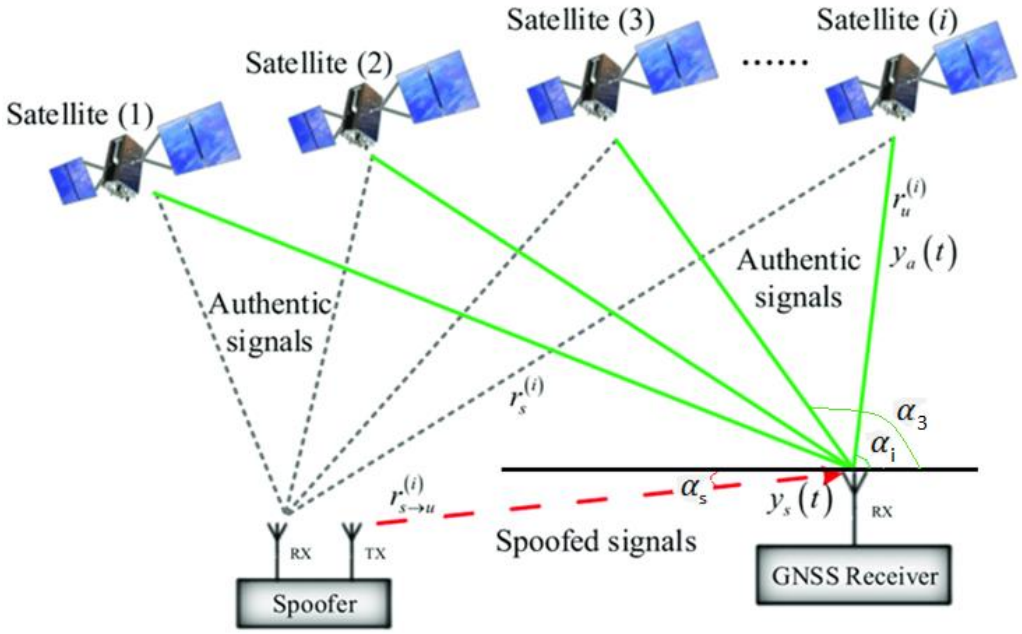
[7] M. L. Psiaki, B. W. O'Hanlon, S. P. Powell, J. A. Bhatti, K. D. Wesson, T. E. Humphreys, A. Schofield, "GNSS spoofing detection using two-antenna differential carrier phase", *Proceedings of the 27th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS +)*, pp. 2776-2800, Sep. 2014.

[8] P. Y. Montgomery, T. E. Humphreys, B. M. Ledvina, "Receiver-autonomous spoofing detection: Experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer", *Proceedings of the International Technical Meeting of The Institute of Navigation*, pp. 124-130, Jan. 2009.

Spoofing Detection – AOA methods

In [6],[9] the authors developed a method called **sum-of-squares (SoS) detector** that:

1. is based on the computation of **Double Difference** carrier-phase measurements;
2. **does not require the estimation of the integer carrier cycles;**
3. **does not require dedicated hardware;**
4. **can be suitable for real-time applications.**



This is the benchmark algorithm for spoofing detection based on AOA defence

[6] D. Borio and C. Gioia. "A dual-antenna spoofing detection system using GNSS commercial receivers", in Proc of ION GNSS+ 2015, Tampa, FL, USA, Sep. 2015, pp.1–6

[9] D. Borio and C. Gioia, "A sum-of-squares approach to GNSS spoofing detection," IEEE Trans. Aerosp. Electron. Syst., vol. 52, no. 4, pp. 1756–1768, Aug. 2016.

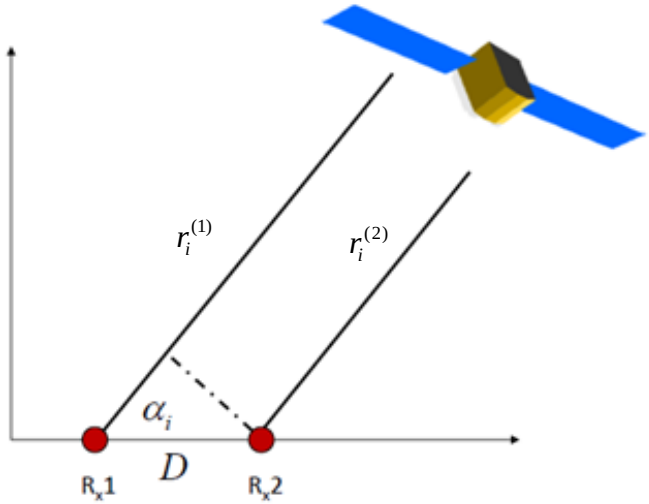
The Sum-of-Squares Method

- When two receivers are synchronized, we can use output data of them to build *single carrier phase differences* for each satellite in common view:

$$\Delta\phi_i = \phi_i^{(1)} - \phi_i^{(2)} = \left(r_i^{(1)} - r_i^{(2)}\right) + \Delta N_i + c\left(\delta T^{(2)} - \delta T^{(1)}\right) + \Delta\varepsilon_i$$

$$r_i^{(1)} - r_i^{(2)} = D\cos(\alpha_i)$$

Distance among the antennas Angle of arrival



- The *double carrier phase difference* (DD) between the *i*-th satellite single difference and the j-th satellite single difference, can be written in terms of unit of cycles as:

$$\Delta\nabla\varphi_i = \frac{1}{\lambda}\left(\Delta\phi_i - \Delta\phi_j\right) = \frac{D}{\lambda}\left(\cos(\alpha_i) - \cos\left(\alpha_j\right)\right) + \Delta\nabla N_i + \Delta\nabla\varepsilon_i$$

The Sum-of-Squares Method

- The term $\left(\cos(\alpha_i) - \cos(\alpha_j)\right)$ of double carrier phase differences can be used to design a statistical test, formulated on the two hypotheses:

$$H_0) \quad \cos(\alpha_i) - \cos(\alpha_j) = 0 \quad \forall(i,j)$$

$$H_1) \quad \exists i,j : \cos(\alpha_i) - \cos(\alpha_j) \neq 0$$

H_0 is the null hypothesis representing **the case of a spoofing attack (same AOA)**

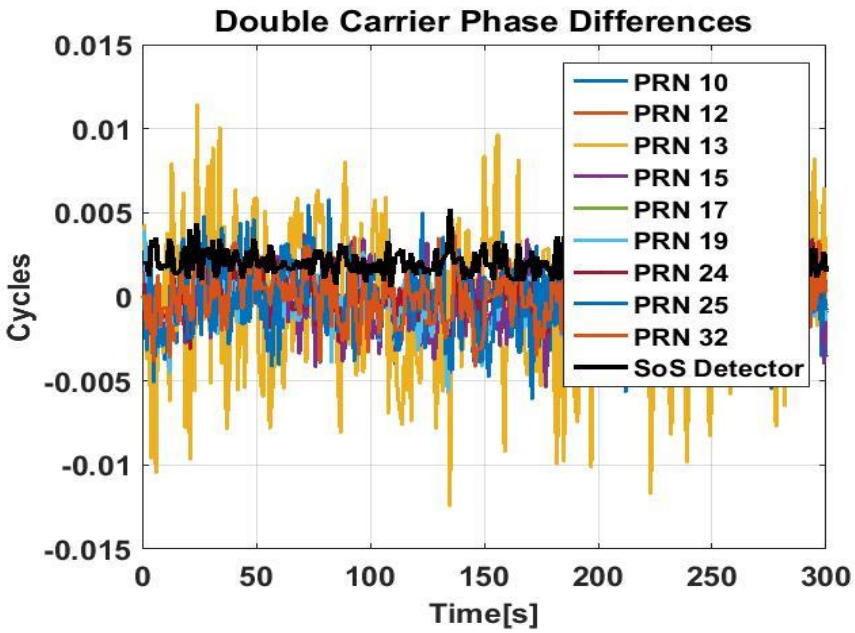
H_1 is the alternative hypothesis which is chosen under **normal operating condition**.

- According to [6] the Generalized Likelihood Ratio Test (GLRT) approach is proposed to discriminate between H_0 and H_1 at each observation epoch, based on the following test statistic:

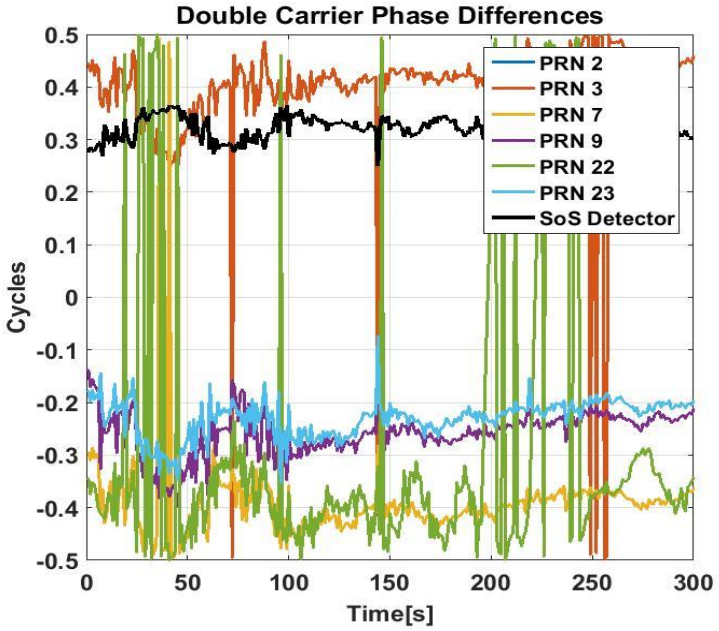
$$\Lambda_{\mathrm{SoS}}(\Delta\nabla\varphi) = \sum_{i=1}^{I} \omega_i [\Delta\nabla\varphi_i - round(\Delta\nabla\varphi_i)]^2$$

The Sum-of-Squares Method
Results and Limitations

RESULTS



Spoofing attack H_0



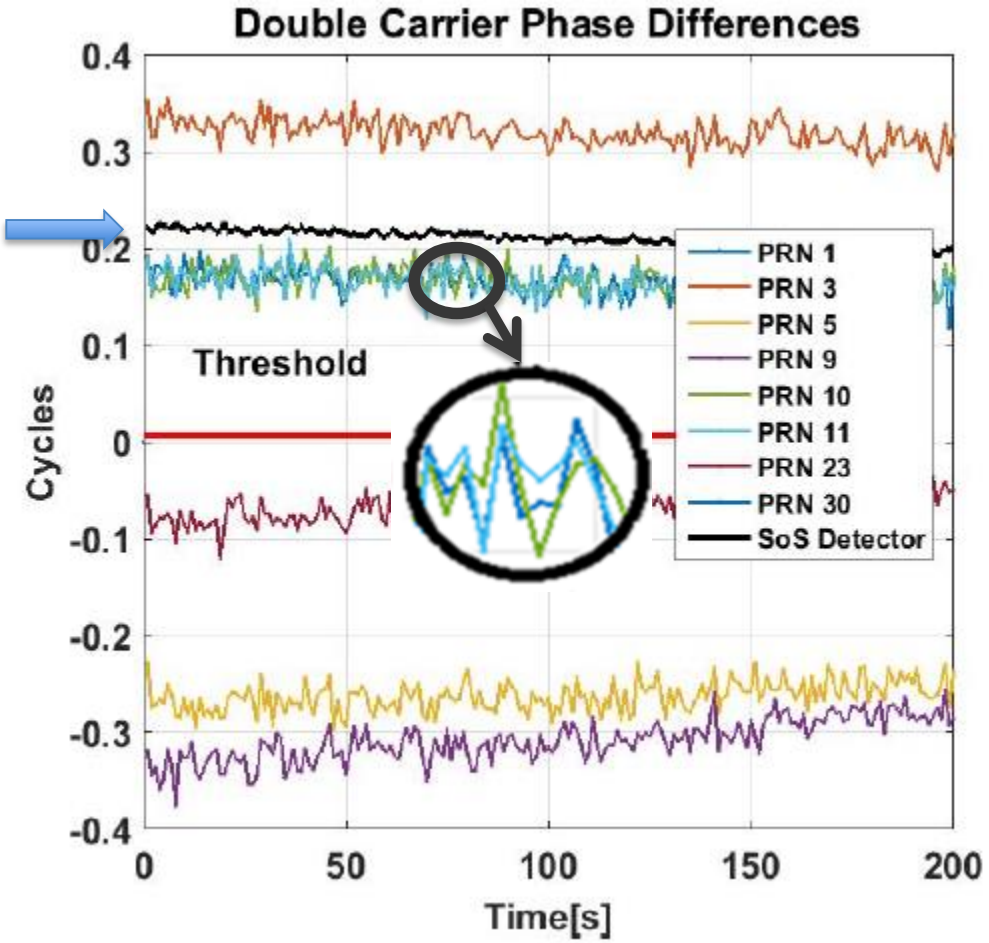
Normal condition H_1

There are two-orders of magnitude of difference between H_1 and H_0 !

The Sum-of-Squares Method Results and Limitations

LIMITATIONS

- Case where the receiver is simultaneously tracking two subsets of signals, namely the authentic and the counterfeit ones.
- In this example the spoofer has generated counterfeit signals for PRNs 1, 10 and 11
- **The SoS detector fails in recognizing the presence of counterfeit signals!**



NEW METHOD BASED ON Dispersion of Double Differences" (D^3)

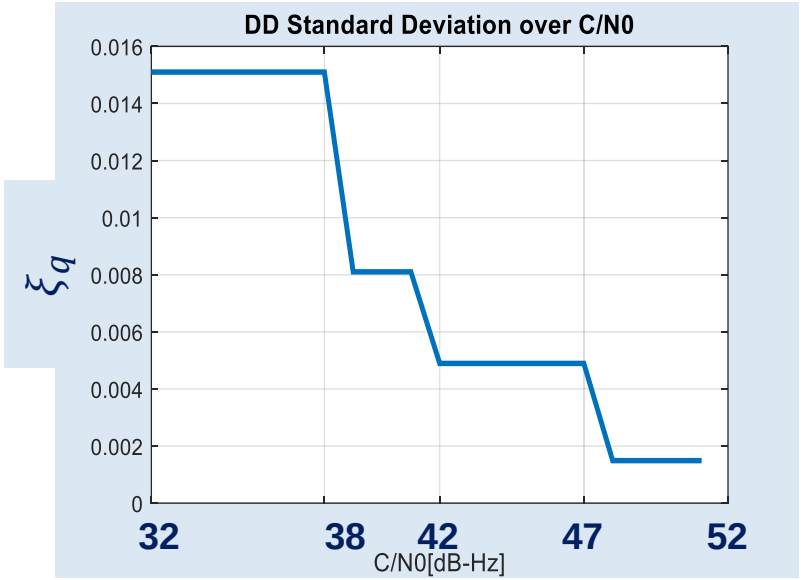
Outline

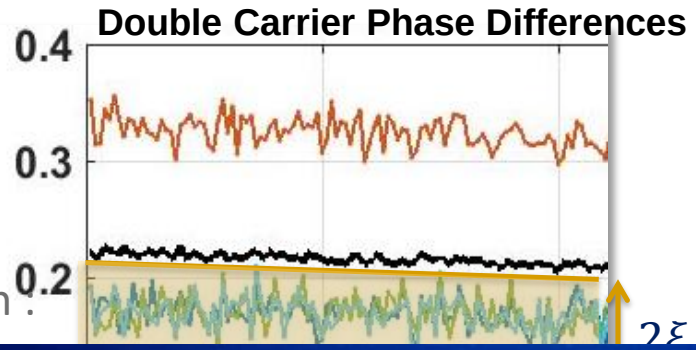
- GNSS Spoofing: Real Events and Main Concepts
- **Spoofing Detection – Angle of Arrival Defence**
  - The Sum-of-Squares Method
  - **The dispersion of the double differences (D^3) Method**
- Spoofing Direction of Arrival (DoA) Estimation
  - A “Precise and Fast” Approach
  - Some tests in the lab & Results
- Conclusions

The dispersion of the double differences (D^3) : spoofing detection algorithm

GENERAL CONCEPTS

1. It is a modification of SoS
2. In order to take the correct decision, the «amount of dispersion» must be quantified:
   - Threshold selection, ξ_q
   - It depends on the Signal-to-Noise Ratio





Details available in [1].

nautec 2018

5 - 7 December 2018 | ESA-ESTEC | The Netherlands

Nguyen V. H., Falco G., Falletti E., Nicola M., **A Dual Antenna GNSS Spoofing Detector Based on the Dispersion of Double Difference Measurements**

The dispersion of the double differences (D^3): spoofing detection algorithm

KEY ELEMENTS

- The fractional DDs associated to the spoofer and the ones related to the true satellites according to a common satellite ***r*** are:

$$\Delta\nabla\varphi_{i,r|FRACT} = \underbrace{\frac{D}{\lambda}\left(\cos(\alpha_i)-\cos(\alpha_r)\right)}_{\mu} + \xi_{q,ir}, \quad \forall i \in Spoofer$$

$$\Delta\nabla\varphi_{l,r|FRACT} = \underbrace{\frac{D}{\lambda}\left(\cos(\alpha_l)-\cos(\alpha_r)\right)}_{\mu_l} + \xi_{q,lr}, \quad \forall l \in Authentic$$

- All the spoofed signals come from the same direction of arrival and their fractional DDs are superimposed → **same mean term μ!**

- We form the "**Regions of Similarity**" $\Sigma_j = \left(\mu_j - \xi_{q,j}, \mu_j + \xi_{q,j}\right)$, for all sat in tracking (j)

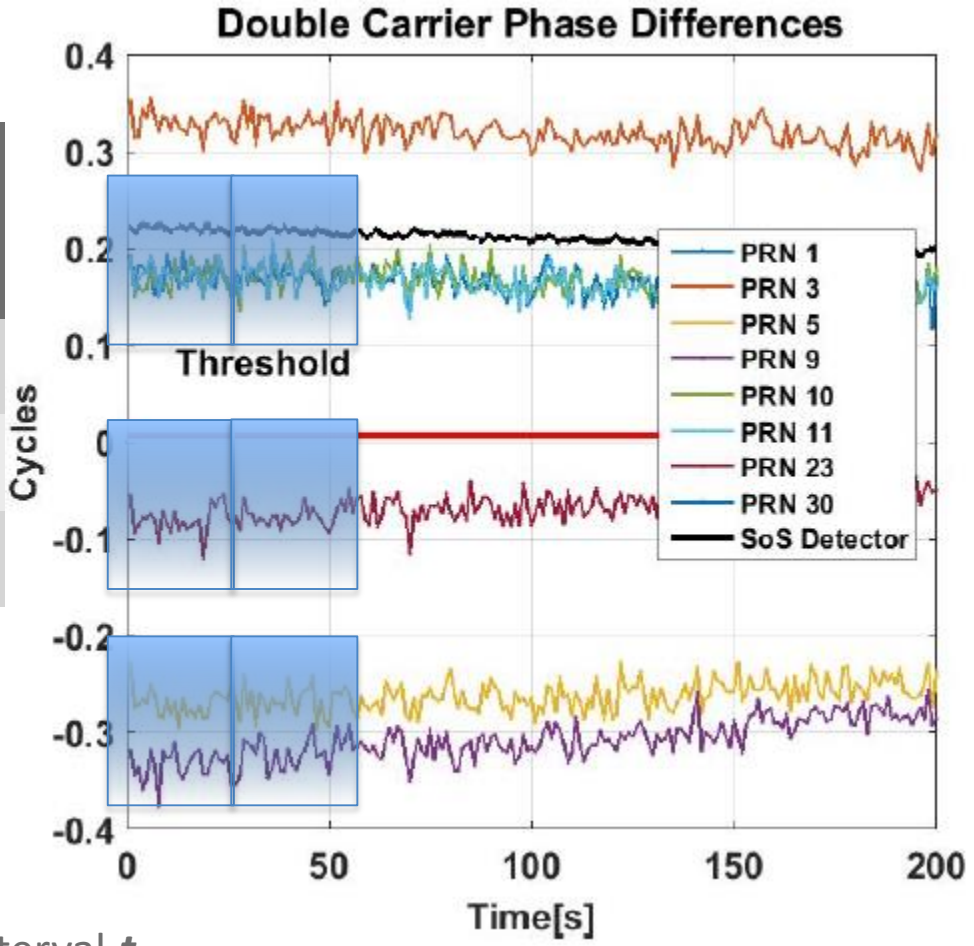
- **A spoofing attack is detected when the number of fractional DDs within one of the regions Σ_j is at least 3**

The dispersion of the double differences (D^3) : spoofing detection algorithm

AN EXAMPLE: 'Mixed' tracking

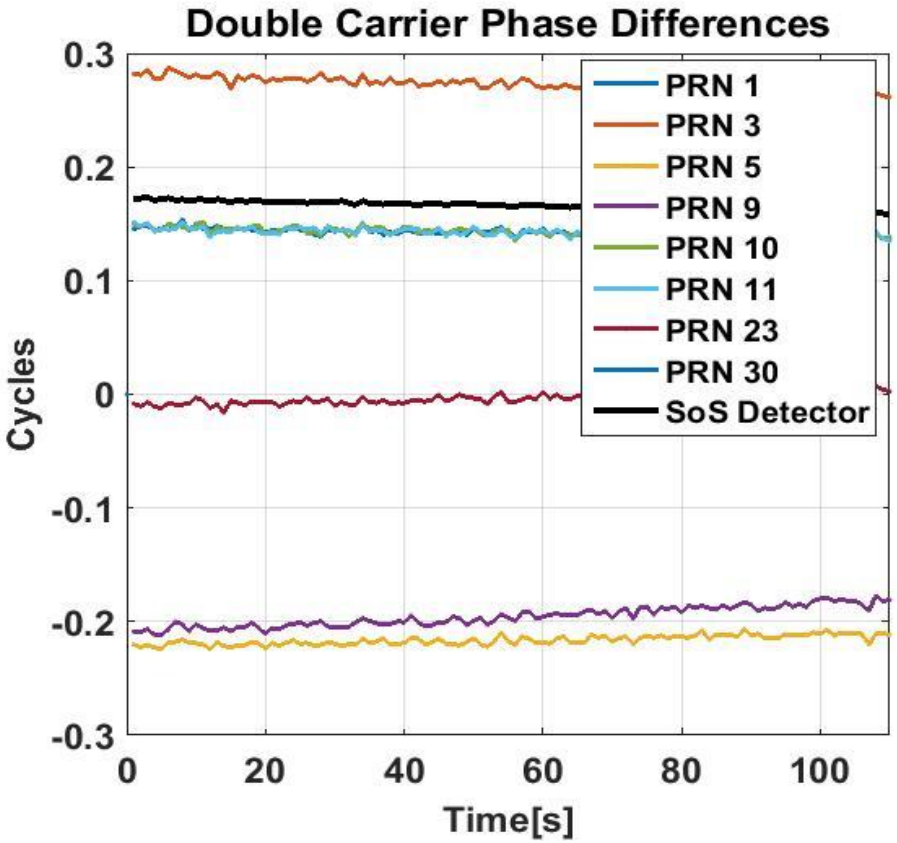
"Regions of Similarity" Σ_j	DDs $\in \Sigma_j$
#1	2
#2	1
#3	**3**

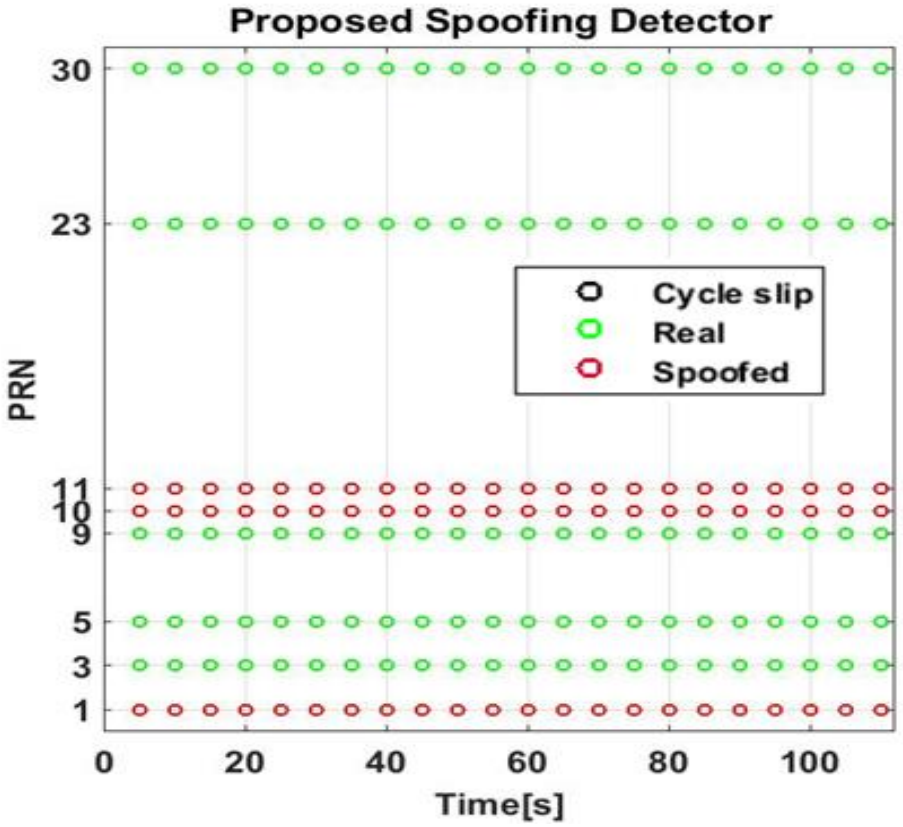
Spoofing attack DETECTED!



- The procedure is repeated at regular time interval ***t***

The dispersion of the double differences (D^3) : spoofing detection algorithm





Method valid for a dual-antenna system:

More antennas => ↓Pfa (probability of false alarm).

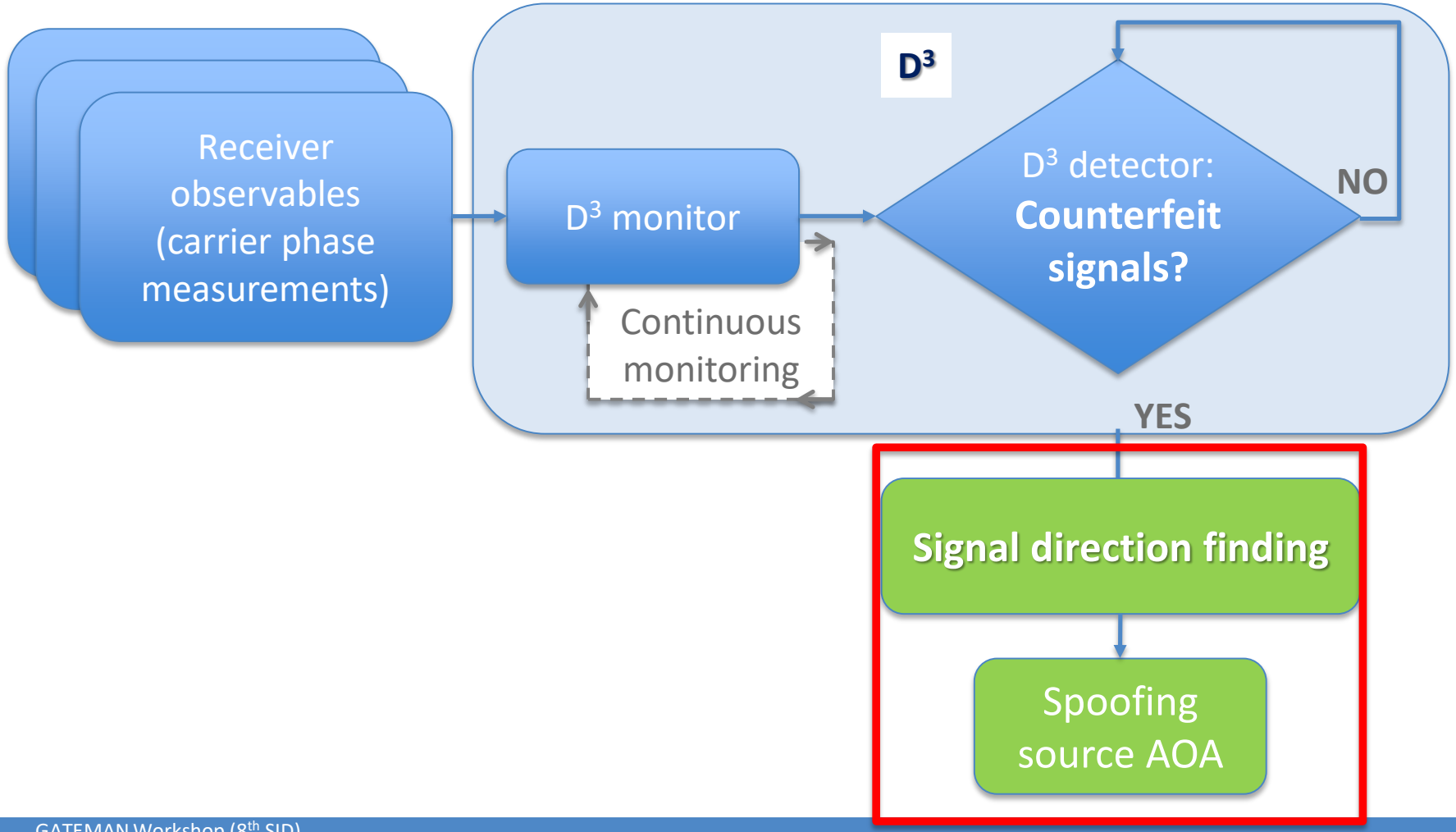
Longer baseline => ↓Pfa (probability of false alarm).

Outline

- GNSS Spoofing: Real Events and Main Concepts
- Spoofing Detection – Angle of Arrival Defence
  - The Sum-of-Squares Method
  - The dispersion of the double differences (D^3) Method
- **Spoofing Direction of Arrival (DoA) Estimation**
  - A “Precise and Fast” Approach
  - Some tests in the lab & Results
- Conclusions

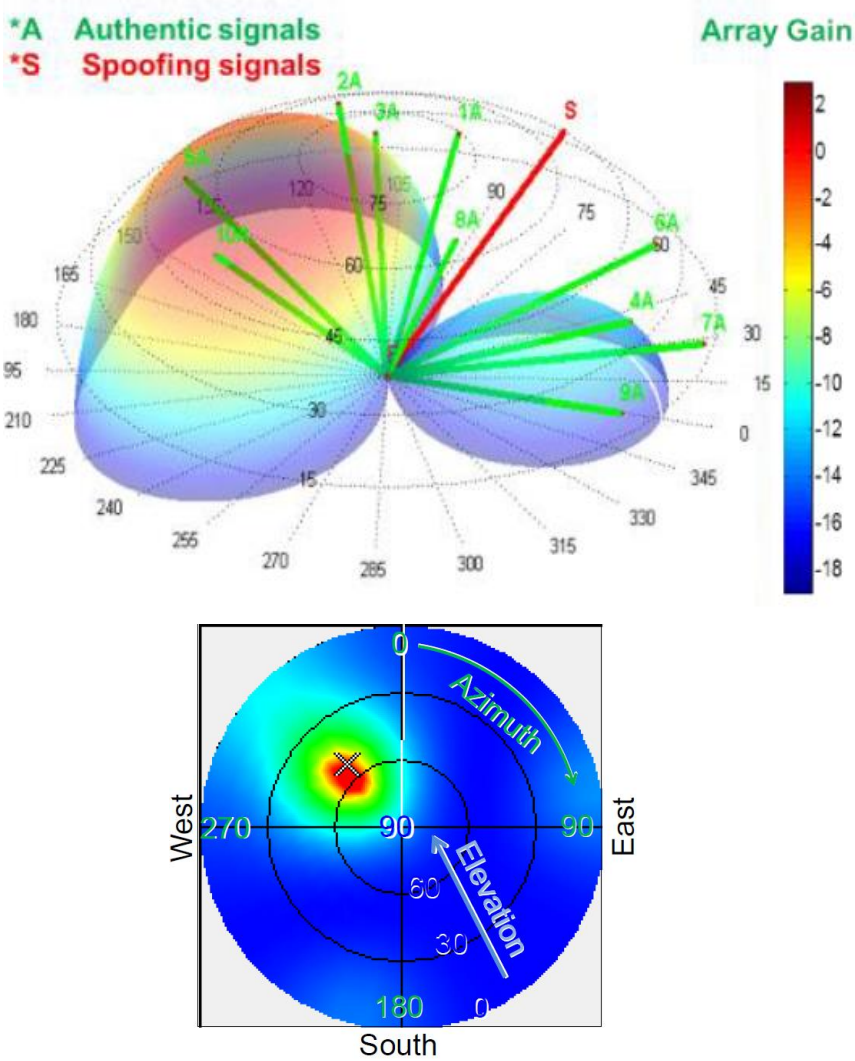
Spoofer's Angle of Arrival Estimation

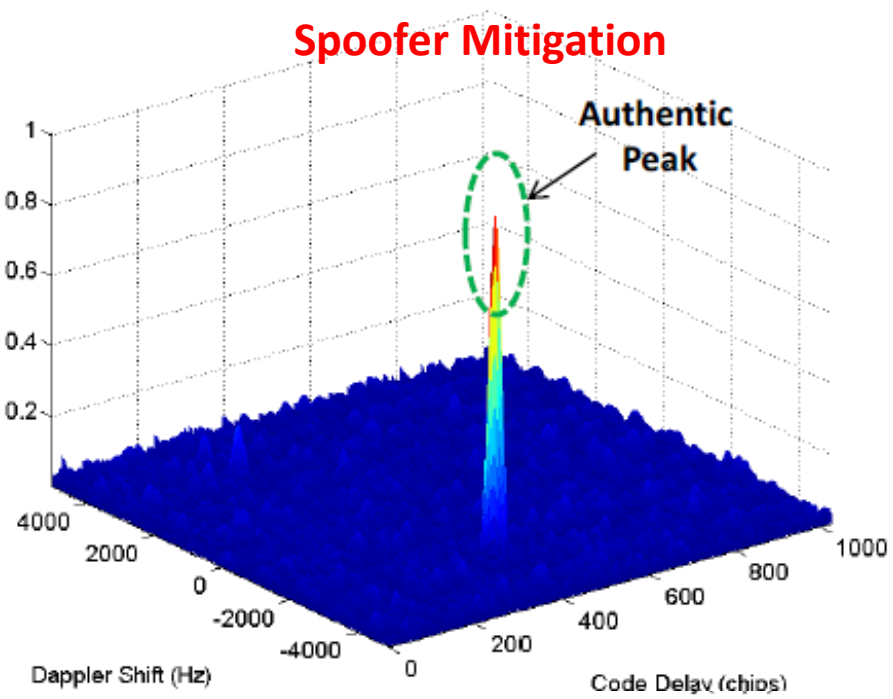
Spoofing detection and signal Direction Finding Logic:



Spoofer's Angle of Arrival+Mitigation

From Theoretical Point of View…





[5] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "GPS spoofer countermeasure effectiveness based on signal strength, noise power and C/N0 observables," International Journal of Satellite Communications and Networking, vol. 30, no. 4, pp. 181–191, 2012.

Spoofer's AoA Estimation

References

WORKING PAPERS

Real World Spoofing Trials and Mitigation via Direction of Arrival Discrimination

This article demonstrates that a synthetic aperture antenna can reliably detect and mitigate even sophisticated spoofing attacks rendered against Global Navigation Satellite Systems. The direction-of-arrival is a reliable metric to discriminate spoofing signals from line-of-sight (LOS) signals and to also localize one or more spoofers with high angular resolution of two degrees.

JÜRGEN DAMPF
IGASPIN GMBH
DR. THOMAS PANY
INSTITUTE OF SPACE TECHNOLOGY AND SPACE APPLICATIONS, UNIVERSITÄT DER BUNDESWEHR MÜNCHEN

Generation and transmission of faked GNSS signals – so-called spoofing – poses a major threat to GNSS. Spoofing has received considerable attention in recent years, but conclusive assessments or proven countermeasures have still not been found. This article summarizes experience gained while conducting real-world spoofing attacks, with one or two transmission antennas. They were conducted using a modified GNSS radio-frequency (RF) signal generator. A reliable countermeasure against spoofing is direction-of-arrival discrimination and

Today many applications rely on GNSS and the number is continuously growing. Some of these applications also incorporate GNSS reference station data to improve their navigation solution. Misleading or degrading a GNSS navigation solution can have serious harmful impacts, especially when thinking about Safety-of-Life services. GNSS spoofing is an intentional attack on a GNSS receiver to mislead or degrade the navigation solution. Spoofing is considered as a serious threat, especially when spoofing GNSS reference stations that distribute their degraded or falsified correction

- Countermeasure against spoofing done through direction-of-arrival (DoA) discrimination
- DoA realized using a rotating GNSS antenna employing synthetic aperture processing and an adaptive beamforming algorithm

✗ It requires a fully SW GNSS receiver in order to acquire and track the spoofed signal

✗ It can be viewed as a variant of a vector tracking receiver (access to the tracking stage is needed)

[10] ÜRGEN DAMPF, DR. THOMAS PANY, WOLFGANG BÄR, JÓN WINKEL, LEOŠ MERVART, JOSÉ-ÁNGEL ÁVILA-RODRÍGUEZ, AND RIGAS IOANNIDES WITH GÜNTER HEIN, "Real World Spoofing Trials and Mitigation Via Direction of Arrival Discrimination," Inside GNSS, June 2017

Spoofer's AoA Estimation

References

THE JOURNAL OF NAVIGATION, Page 1 of 19. © The Royal Institute of Navigation 2013
doi:10.1017/S0373463313000453

Precise and Fast GNSS Signal Direction of Arrival Estimation

Rui Sun[1], Kyle O'Keefe[2], Jian Guo[1] and Eberhard Gill[1]

[1](*Department of Space Engineering, Faculty of Aerospace Engineering, Delft University of Technology, Kluyerweg 1, Delft, 2629HS, The Netherlands*)
[2](*Department of Geomatics Engineering, Schulich School of Engineering, University of Calgary, 2500 University Dr. NW, Calgary, Alberta, T2N 1N4, Canada*)
(E-mail: j.guo@tudelft.nl)

This paper proposes a precise and fast direction of arrival estimation method using Global Navigation Satellite System (GNSS) carrier phase measurements. Single-epoch, single-satellite integer cycle ambiguities are reliably resolved by making use of constraints and taking advantages of antenna arrays. The algorithm shows good robustness in cases where signal interruption or corruption occurs on some antenna elements as long as four antenna elements in a non-planar array have uncorrupted observables. The algorithm is demonstrated by field tests where antenna elements are connected to multiple receivers with an external common clock. The results indicate a high success rate of single-epoch ambiguity resolution and high direction of arrival accuracy.

KEY WORDS

1. Signal direction of arrival. 2. Ambiguity resolution. 3. Constraint. 4. Antenna array.

Submitted: 4 April 2013. Accepted: 28 June 2013.

1. INTRODUCTION. Global Navigation Satellite System (GNSS) observables include non-ambiguous but coarse pseudoranges and precise but ambiguous carrier phases. For precise applications, carrier phases must be used while the pseudorange may help to solve the integer cycle ambiguities. Applications include, e.g., kinematic positioning (Hada, et al., 2000; Parkins, 2011), static surveying (Leick, 2004) and attitude determination (Teunissen, 2007; Giorgi and Teunissen, 2012). The GNSS signal Direction of Arrival (DOA) can also be estimated using carrier phase measurements. This requires multiple antennas or an antenna array fixed on a rigid platform. Many applications need an accurate estimate of DOAs. For example, DOAs are crucial to allow beamforming with antenna arrays in the presence of interference or multipath. The signal directions need to be available so that various antenna elements can be manipulated to allow the main beam to be pointed towards the

- The paper's target is the estimation of the DoA of each satellite in view (not only the spoofer)
- It exploits the generation of SINGLE DIFFERENCES of carrier–phase measurements
- Integer ambiguities need to be solved before estimating the DoA

This method is suitable to be used in GATEMAN! (no GNSS fully SW is necessary)!

Only slight modifications are needed to estimate the DoA of the spoofer!

[11]R. Sun, K. O'Keefe, J. Guo, E. Gill, Precise and Fast GNSS Signal Direction of Arrival Estimation. THE JOURNAL OF NAVIGATION, Page 1 of 19. © The Royal Institute of Navigation 2013. doi:10.1017/S0373463313000453.

Outline

- GNSS Spoofing: Real Events and Main Concepts
- Spoofing Detection – Angle of Arrival Defence
  - The Sum-of-Squares Method
  - The dispersion of the double differences (D^3) Method
- **Spoofing Direction of Arrival (DoA) Estimation**
  - **A "Precise and Fast" Approach**
  - Some tests in the lab & Results
- Conclusions

Spoofer's AoA Estimation

Direction finding: "Precise & Fast" Algorithm (PAF)

Adaptation to the GATEMAN context

Principle: resolve the projection of the known antenna baselines onto the ***signal DOA***, contained in the ***single differenced*** carrier phase observables:

single carrier phase differences for each satellite in common view

$$\Delta\phi_i = \phi_i^{(\mathrm{RX2})} - \phi_i^{(\mathrm{RX1})}, \quad i\text{-th satellite}$$

single carrier phase differences for each satellite in common view

$$\Delta\phi_i = \mathbf{g}^{(12),T} \cdot \mathbf{x}_i + \lambda\Delta N_i^{(12)} + \Delta b^{(12)} + \Delta\varepsilon_\phi, \quad i\text{-th satellite}$$

measured

carrier SD

baseline 1-2

known

DOA:

$\mathbf{x}_i = (x_i, y_i)^T$

integer ambiguity

other errors

random uncertanties

clock/cable bias

known after calibration (receivers synchronized) and removed

Spoofer's AoA Estimation

Direction finding: "Precise & Fast" Algorithm (PAF)

Adaptation to the GATEMAN context

1. Put together:

- SD code range measurements
- SD carrier phase measurements
- Two frequencies (optional)
- Two baselines

Under the hypothesis of **single DOA** for all the signals (i.e., *M* spoofed signals only)

$$\begin{bmatrix} \Delta\mathbf{P}^1 \\ \vdots \\ \Delta\mathbf{P}^M \\ \Delta\boldsymbol{\Phi}_{f1}^1 \\ \vdots \\ \Delta\boldsymbol{\Phi}_{f1}^M \\ \Delta\boldsymbol{\Phi}_{f2}^1 \\ \vdots \\ \Delta\boldsymbol{\Phi}_{f2}^M \end{bmatrix} = \begin{bmatrix} \mathbf{G}^T & & & 0 & & \\ \vdots & & & & & \\ \mathbf{G}^T & & & & & \\ \mathbf{G}^T & \lambda_{f1} & & & & \\ \vdots & & \ddots & & & 0 \\ \mathbf{G}^T & & & \lambda_{f1} & & \\ \mathbf{G}^T & & & & \lambda_{f2} & \\ \vdots & & 0 & & & \ddots \\ \mathbf{G}^T & & & & & \lambda_{f2} \end{bmatrix} \cdot \begin{bmatrix} \mathbf{x} \\ \Delta\boldsymbol{N}_{f1}^1 \\ \vdots \\ \Delta\boldsymbol{N}_{f1}^M \\ \Delta\boldsymbol{N}_{f2}^1 \\ \vdots \\ \Delta\boldsymbol{N}_{f2}^M \end{bmatrix} + \Delta\boldsymbol{\varepsilon} \quad \in R^{6M\times 1}, \qquad \textit{subject to } \|\mathbf{x}\| = 1$$

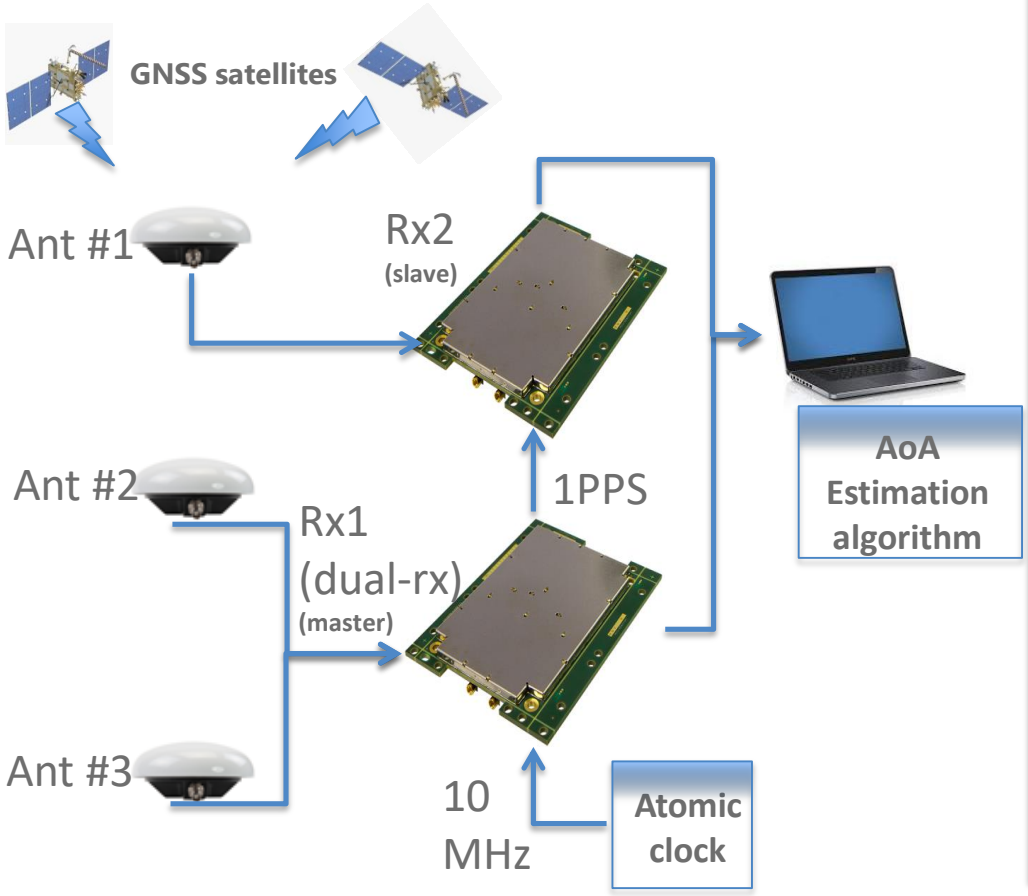
2. Then resolve using the PAF approach

Outline

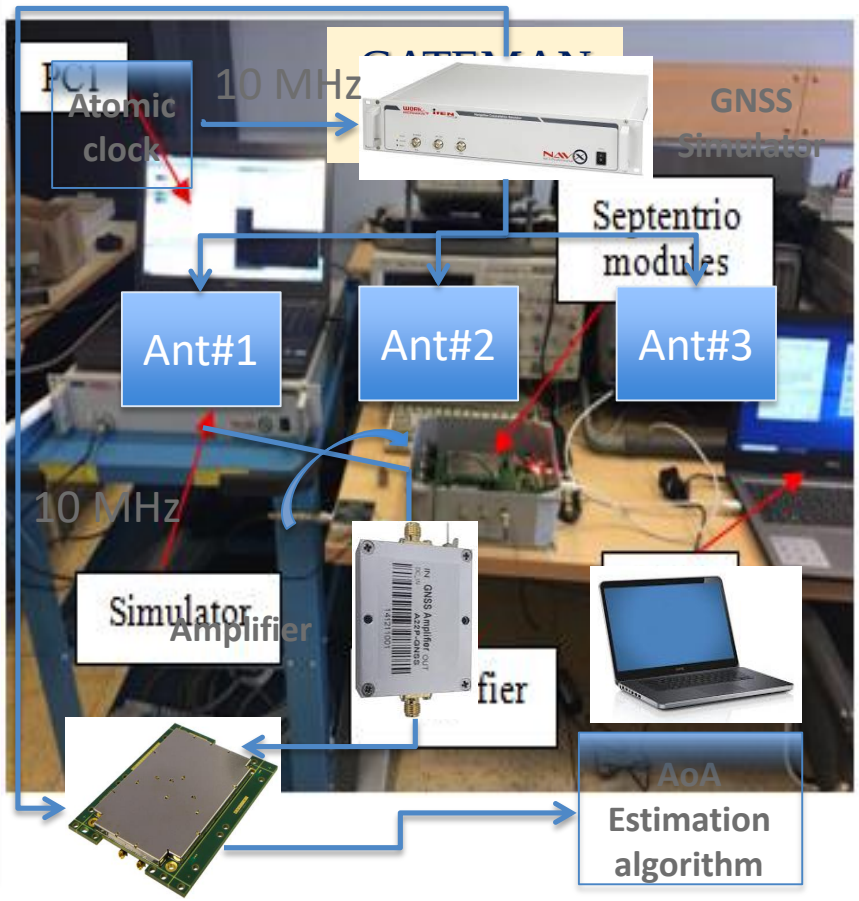
- GNSS Spoofing: Real Events and Main Concepts
- Spoofing Detection – Angle of Arrival Defence
  - The Sum-of-Squares Method
  - The dispersion of the double differences (D^3) Method
- **Spoofing Direction of Arrival (DoA) Estimation**
  - A “Precise and Fast” Approach
  - **Some tests in the lab & Results**
- Conclusions

Spoofer's AoA Estimation
In-lab algorithm verification

HW equipment setup (on the field)

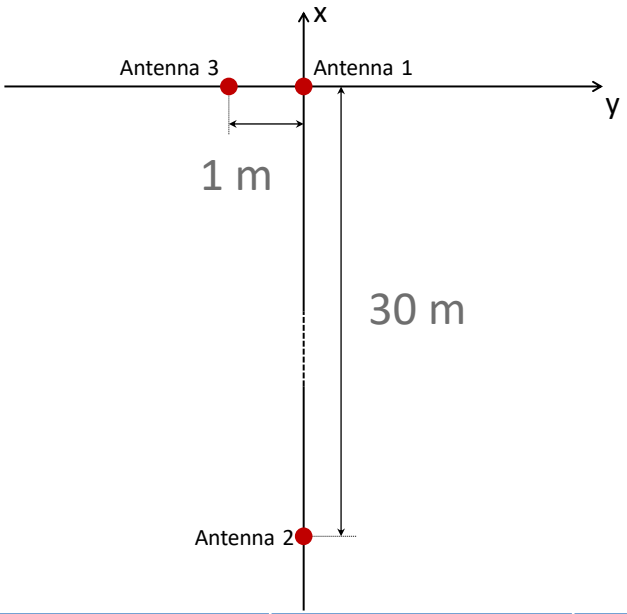


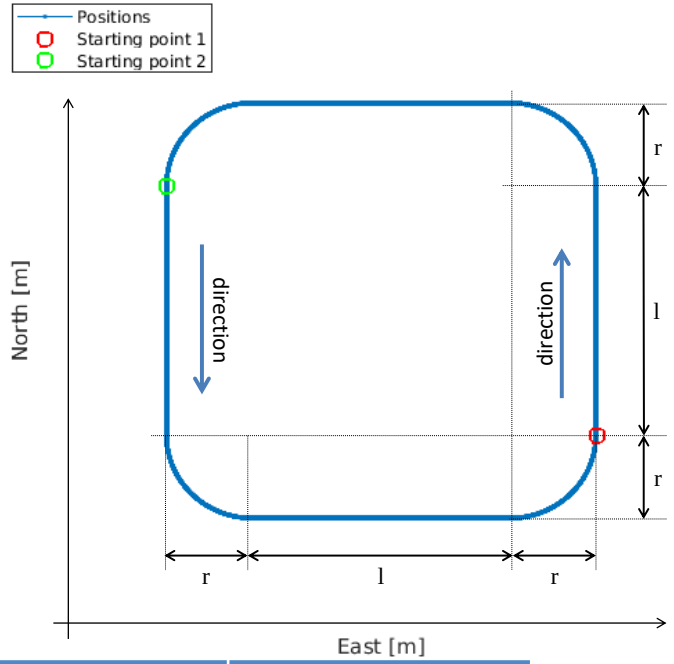
In-lab equipment setup



Spoofer's AoA Estimation
In-lab algorithm verification

Antenna positions and simulated aircraft trajectories



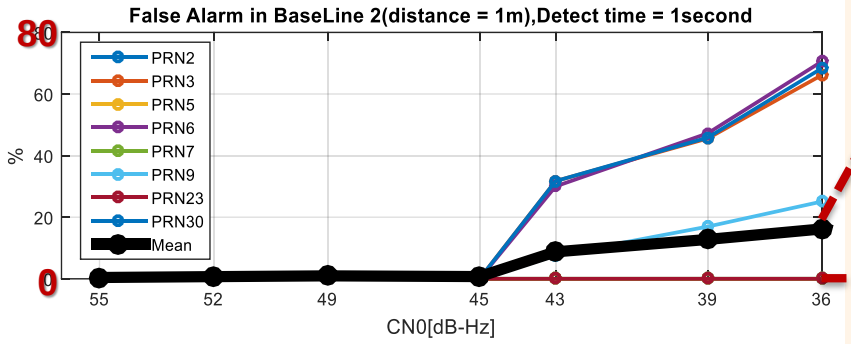


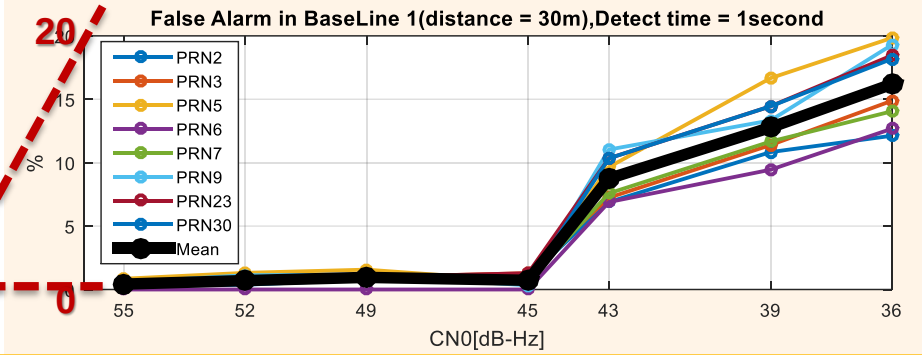
Trajectory name	Side Length (l)	Turn radius (r)	Velocity	Starting point
TRJ1	15 km	5 km	250 km/h	Starting point 1
TRJ2	30 km	10 km	500 km/h	Starting point 2

Spoofer's AoA Estimation
In-lab algorithm verification

- Effects of the length of the baseline on the Detection algorithm

Baseline 1 m | **Baseline 30 m**





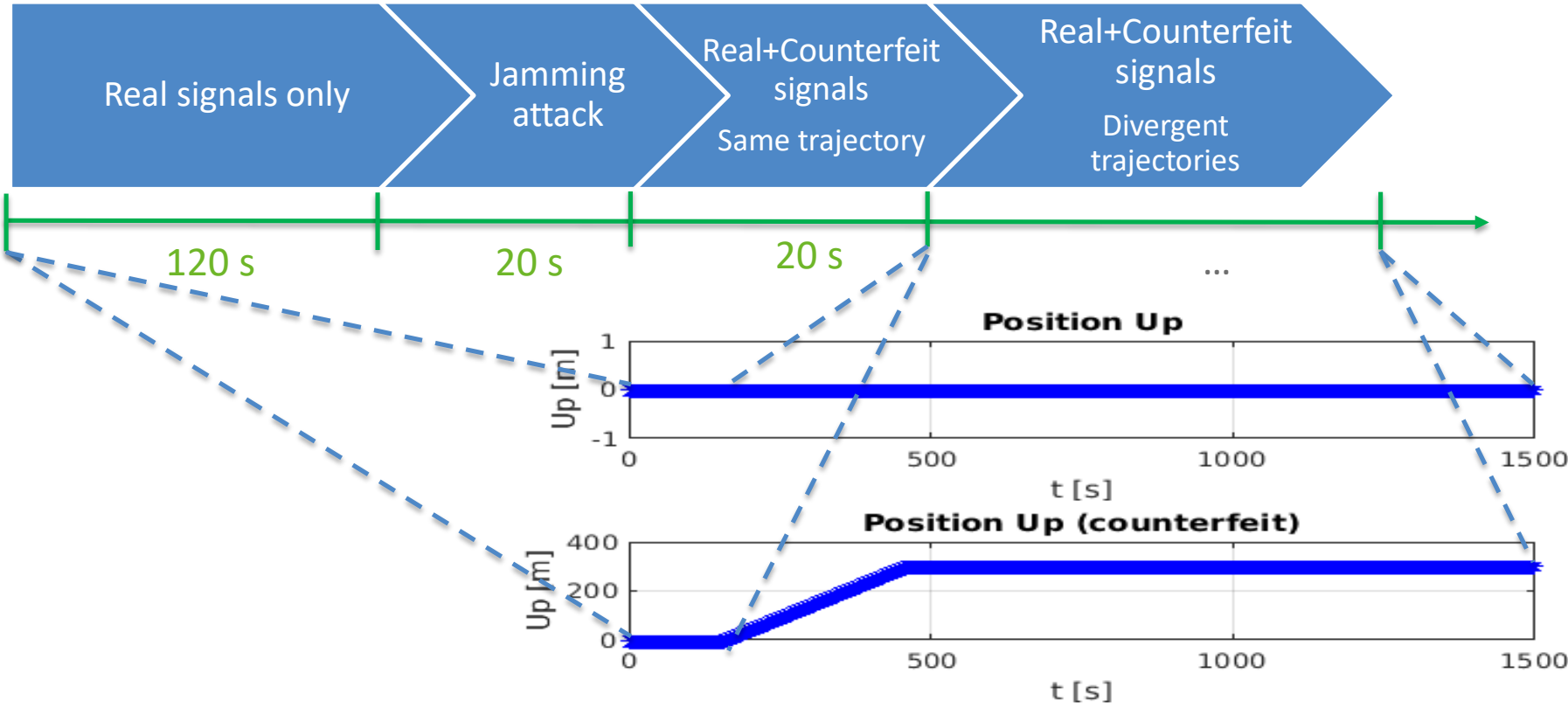
- Effects of the length of the baseline on the AoA algorithm

Test case \ Length	Baseline b1	Baseline b2
SPO-TC-03.2	30 m	1 m
SPO-TC-03.2b	3 m	1 m
SPO-TC-03.2c	5 m	1 m

Test case	Scenario	Trajectory	Tracking status	DOA Availability(1) (%)	Correct detection rate(2) (%)	AOA errors (deg)	
						Mean	STD
SPO-TC-03.2	GP-L1x-JS-10-Aemu_02	TRJ2	Complete	66.1	90.5	**5.5**	**8.8**
SPO-TC-03.2b	GP-L1x-JS-10-Aemu_02b	TRJ2	Complete	66.1	90.5	**5.5**	**8.8**
SPO-TC-03.2c	GP-L1x-JS-10-Aemu_02c	TRJ2	Complete	66.1	91.4	**5.7**	**6.4**

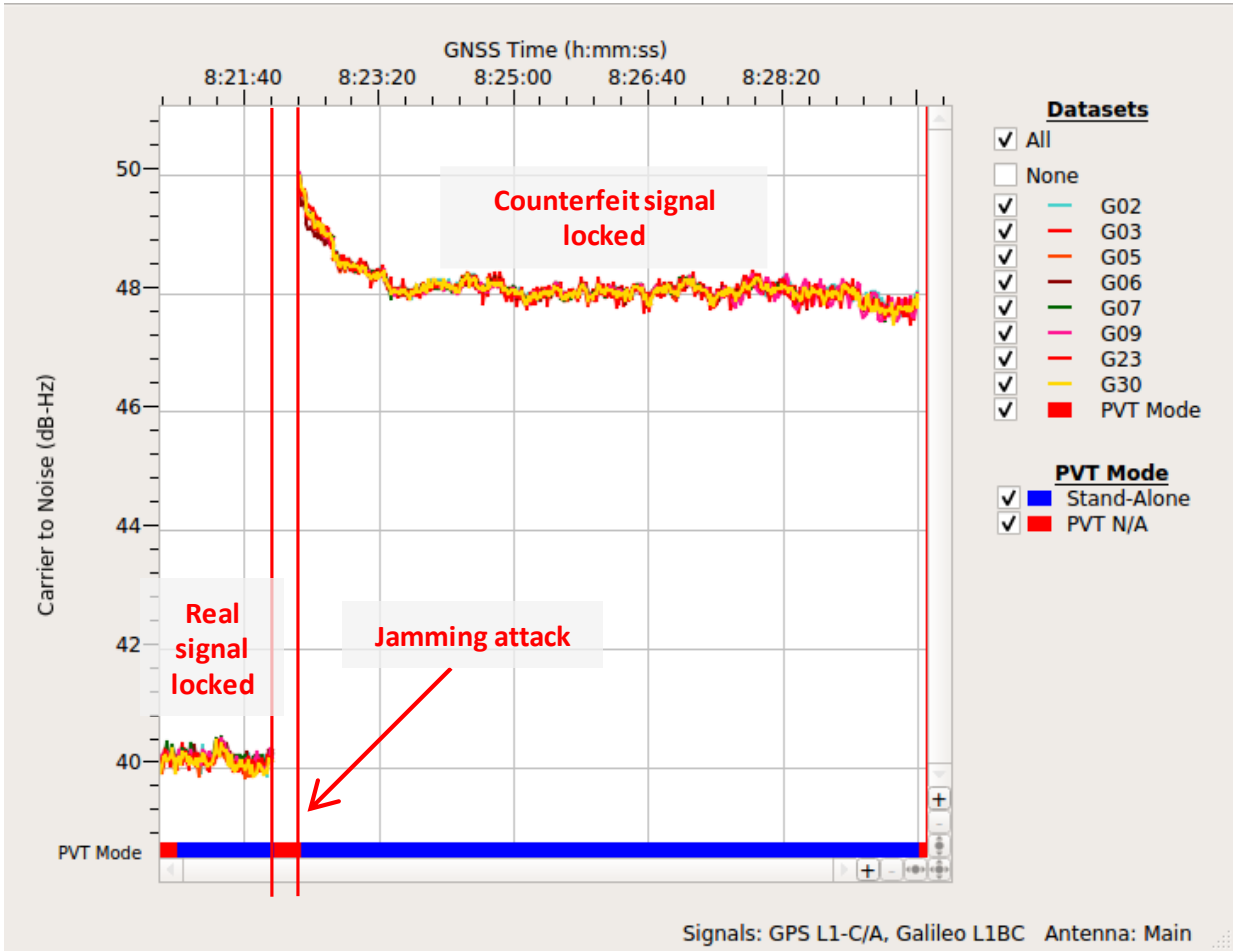
Spoofer's AoA Estimation
In-lab algorithm verification

Simulated spoofing attacks: jamming +(simplistic) spoofing



Spoofer's AoA Estimation
In-lab algorithm verification

jamming +(simplistic) spoofing



Spoofer's AoA Estimation
In-lab algorithm verification

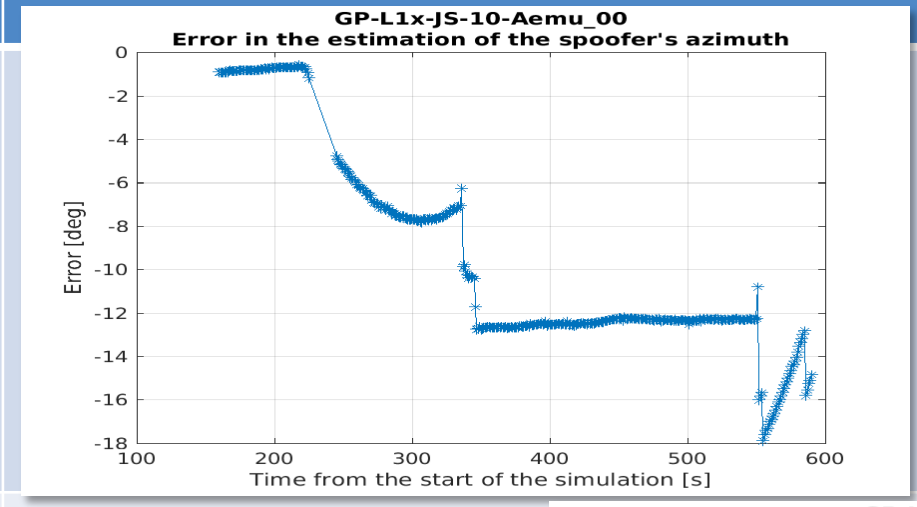
List of test cases

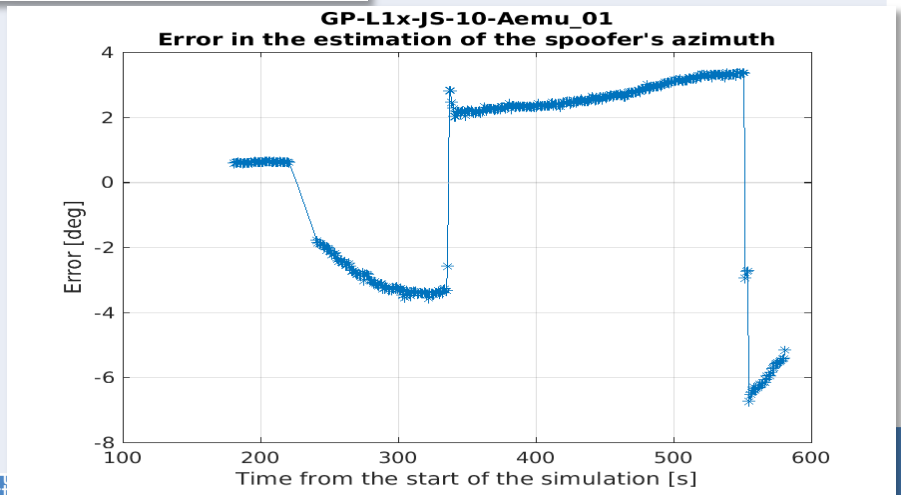
Name	Trajectory	Generated signals (real)	Generated signals (counterfeit)	Target tracking status
GP-L1x-JS-10-Aemu_00	TRJ1	GPS L1 CA	GPS L1 CA	Complete
GP-L1x-JS-10-Aemu_01	TRJ1	GPS L1 CA	GPS L1 CA (incomplete)	Mixed
GP-L1x-JS-10-Aemu_02	TRJ2	GPS L1 CA	GPS L1 CA	Complete
GP-L1x-JS-10-Aemu_03	TRJ2	GPS L1 CA	GPS L1 CA (incomplete)	Mixed
GG-L1x-JS-10-Aemu_00	TRJ1	GPS L1 CA Galileo E1 B/C	GPS L1 CA	Mixed
GG-L1x-JS-10-Aemu_01	TRJ1	GPS L1 CA Galileo E1 B/C	Galileo E1 B/C	Mixed
GG-L1x-JS-10-Aemu_02	TRJ2	GPS L1 CA Galileo E1 B/C	GPS L1 CA	Mixed
GG-L1x-JS-10-Aemu_03	TRJ2	GPS L1 CA Galileo E1 B/C	Galileo E1 B/C	Mixed

Spoofer's AoA Estimation
In-lab algorithm verification

Name	Trajectory	Real signals	Counterfeit signals	Tracking status
GP-L1x-JS-10-Aemu_00	TRJ1	GPS L1 CA	GPS L1 CA	Complete
GP-L1x-JS-10-Aemu_01	TRJ1	GPS L1 CA	GPS L1 CA (incomplete)	Mixed

Examples of receiver outputs





Spoofer's AoA Estimation
In-lab algorithm verification

DOA estimation error statistics

	Scenario	Trajectory type	Tracking type	DOA Availability (%)	DOA Error [RMSE] (deg)	Error percentiles (deg)			
						50th	67th	90th	95th
GPS only	GP-L1x-JS-10-Aemu_00	TRJ1	Complete	89.6	10.6	12.3	12.4	12.7	15.5
	GP-L1x-JS-10-Aemu_01	TRJ1	Mixed	83	3.0	2.7	3.1	3.4	5.6
	GP-L1x-JS-10-Aemu_02	TRJ2	Complete	66.1	6.3	7	7	7.1	7.2
	GP-L1x-JS-10-Aemu_03	TRJ2	Mixed	41.3	1.2	1.3	1.4	1.4	1.4
GPS + Galileo	GG-L1x-JS-10-Aemu_00	TRJ1	Mixed	63.9	5.3	5.5	5.9	7.8	7.9
	GG-L1x-JS-10-Aemu_01	TRJ1	Mixed	42.2	7.5	7.7	7.8	8.4	8.8
	GG-L1x-JS-10-Aemu_02	TRJ2	Mixed	25.7	0.4	0.1	0.1	0.2	0.2
	GG-L1x-JS-10-Aemu_03	TRJ2	Mixed	19.1	3.6	3.6	3.6	3.7	3.7

Outline

- GNSS Spoofing: Real Events and Main Concepts
- Spoofing Detection – Angle of Arrival Defence
  - The Sum-of-Squares Method
  - The dispersion of the double differences (D^3) Method
- Spoofing Direction of Arrival (DoA) Estimation
  - A “Precise and Fast” Approach
  - Some tests in the lab & Results
- **Conclusions**

Conclusions

- **Simulation of realistic spoofing attacks (jamming+ spoofing)**

- **The Detection and direction finding algorithm (DDF) has been successfully tested in case of:**
  - **Multi-constellation system (GPS+GALILEO)**
  - **Different speed of the target user (250-500 km/h)**
  - **Mixed or complete spoofed signals**
  - **Multi-frequency system (L1+L5)**

GATEMAN

Thank you very much for your attention!

This project has received funding from the SESAR Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement No [number]

SESAR JOINT UNDERTAKING

Founding Members

EUROPEAN UNION EUROCONTROL