TESTING ADAPTIVE ANTENNA ARRAYS FOR GNSS RECEIVERS

Markus Irsigler
Product Manager

Sebastian Kehl-Waas
Application Engineer

ROHDE&SCHWARZ

Make ideas real

CONTENTS

SOURCES OF GNSS SIGNAL DEGRADATION
OVERVIEW

Satellite payload

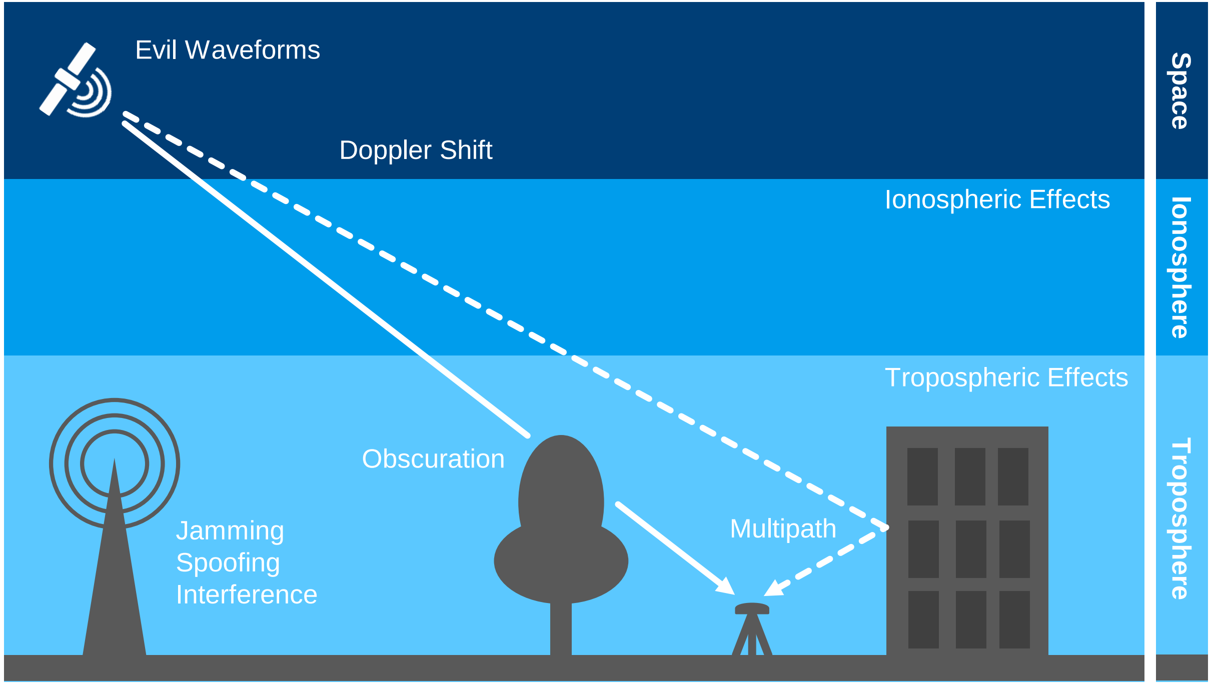
- Evil waveforms

Degradation along signal path

- Ionospheric influences
- Tropospheric influences
- Doppler shift

User environment / man-made threats

- Signal obscuration
- Multipath
- Jamming
- Interference
- Spoofing



SOURCES OF GNSS SIGNAL DEGRADATION
CLASSIFICATION OF MAN-MADE THREATS

GNSS Interference

Interference

Intentional - Jamming -
- Brute-force jamming
- Systematic jamming

Unintentional
- Signal obstruction
- Multipath
- Coexistence

Used signals

Intentional:
- CW interferers
- Broadband noise
- Frequency sweeps
- Pulsed interference
- **Example:** PPD

Unintentional:
- Comm. signals
- Radar signals
- **Examples:**
  - DME/TACAN
  - LTE

SOURCES OF GNSS SIGNAL DEGRADATION
CLASSIFICATION OF MAN-MADE THREATS

GNSS Interference

Interference

- **Intentional - Jamming -**
  - Brute-force jamming
  - Systematic jamming
- **Unintentional**
  - Signal obstruction
  - Multipath
  - Coexistence

Spoofing

- **Broadcast forged GNSS signal**
- **Rebroadcast GNSS signal - Meaconing -**

Used signals

Intentional - Jamming -:

- CW interferers
- Broadband noise
- Frequency sweeps
- Pulsed interference
- **Example:** PPD

Unintentional:

- Comm. signals
- Radar signals
- **Examples:**
  - DME/TACAN
  - LTE

Spoofing:

- GNSS signals generated by signal generator
- Rebroadcast delayed version of live GNSS signals
- Replay prerecorded GNSS signals

SOURCES OF GNSS SIGNAL DEGRADATION
CLASSIFICATION OF MAN-MADE THREATS

GNSS Interference

Interference

Intentional - Jamming -
- Brute-force jamming
- Systematic jamming

Unintentional
- Signal obstruction
- Multipath
- Coexistence

Spoofing

Broadcast forged GNSS signal

Rebroadcast GNSS signal - Meaconing -

Used signals

Intentional:
- CW interferers
- Broadband noise
- Frequency sweeps
- Pulsed interference
- **Example:** PPD

Unintentional:
- Comm. signals
- Radar signals
- **Examples:**
  - DME/TACAN
  - LTE

Spoofing:
- GNSS signals generated by signal generator
- Rebroadcast delayed version of live GNSS signals
- Replay prerecorded GNSS signals

→ Denial of Service | Degraded DUT perf. | Incorrect position/timing information, no reliable navigation

JAMMING AND SPOOFING
A SELECTION OF HEADLINES

GPS Jamming and Spoofing On the Rise

Russia responsible for massive satellite system spoofing, study finds

Thousands of GNSS jamming and spoofing incidents reported in 2020

GPS disruption is a growing problem for aviation

GPS spoofing threatens safety of navigation

Manipulated GPS data becomes a billion-dollar risk for logistics

GPS Jamming Still Causing Problems in Finnmark

GPS interference and jamming on the increase

The growing problem of jamming and spoofing of GPS satellite navigation signals just keeps getting worse

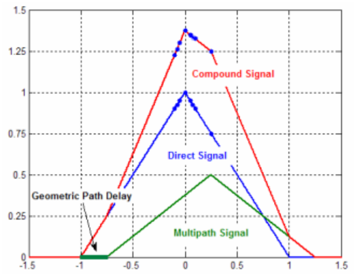
INTERFERENCE DETECTION AND MITIGATION
OVERVIEW

Interference Detection

- AGC monitoring
- Spectrum monitoring
- C/N_0 monitoring
- Analysis of GNSS observables
  - Single- and double differencing
  - “Code minus carrier” (CMC) processing
- PVT monitoring, RAIM
- Multicorrelator techniques

Interference Mitigation

- Frequency domain adaptive filtering
- Pulse blanking
- Optimized antenna reception pattern, e.g. choke ring antennas



from: everythingrf.com

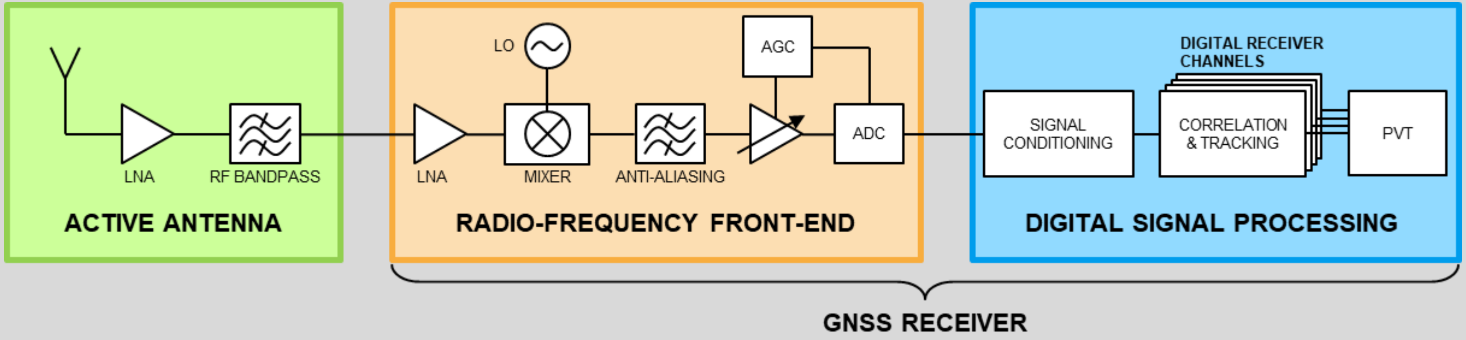
INTERFERENCE DETECTION AND MITIGATION
SINGLE-ANTENNA GNSS RECEIVER

RX Functions

GNSS signal reception and band limitation

Amplification, down-conversion to IF/BB, automatic gain control, analog-digital conversion

Signal conditioning, correlation & tracking, position-velocity-time (PVT) solution



Detection

- AGC monitoring

- Spectrum monitoring
- C/N_0 and PVT monitoring
- Analysis of GNSS observables, RAIM
- Multicorrelator techniques

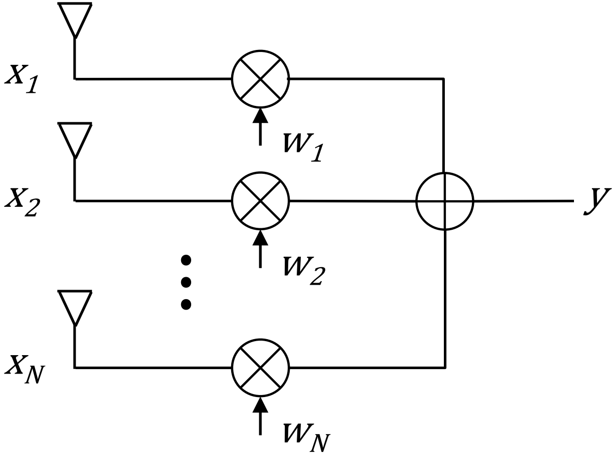
Mitigation

- Optimized antenna reception pattern
- Out-of-band filtering

- Frequency domain adaptive filtering
- Pulse blanking

CONTENTS

ADAPTIVE ANTENNA ARRAYS IN GNSS



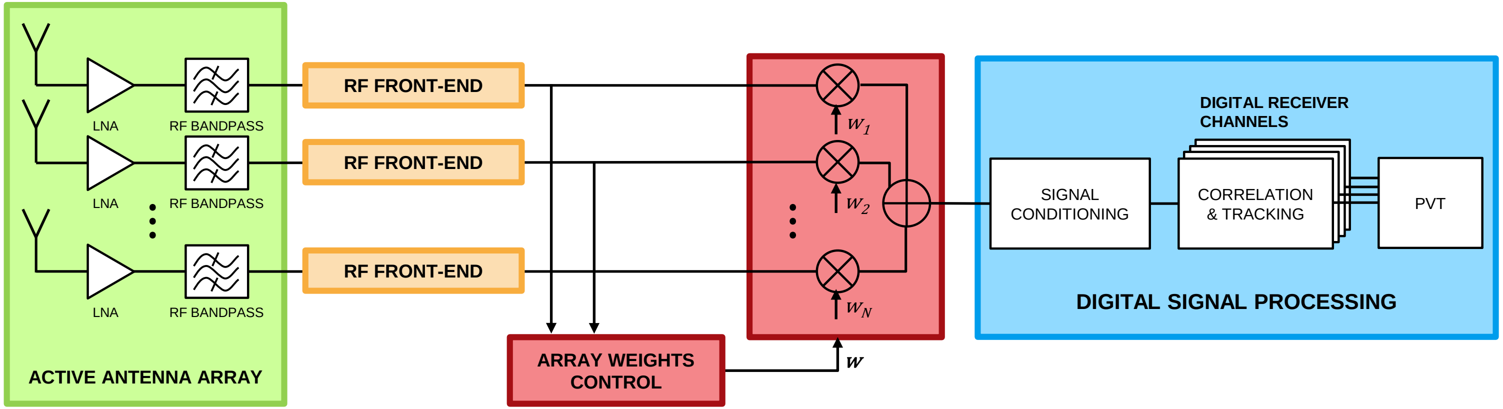
- Electronically steered antenna reception pattern based on applying complex weights $\boldsymbol{w}$ on the receive signal on each antenna element $\boldsymbol{x}$:

$$y = \boldsymbol{w}^H \boldsymbol{x}\,, \qquad \text{where } \boldsymbol{w} = \begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_N \end{bmatrix} \text{ and } \boldsymbol{x} = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_N \end{bmatrix}$$

- Weights are calculated based on optimization criteria
- Possible at pre- or post-correlation stage
- Typical optimization criteria:
  - Minimize output power (*Null-steering*)
  - Maximize signal to interference and noise ratio (SINR) (*Beamforming*)
- Also known as controlled reception pattern antenna (CRPA)

ADAPTIVE ARRAY SIGNAL PROCESSING
PRE-CORRELATION TECHNIQUES (1)

- Typical architecture:



- GNSS signals are received well below the noise floor
- Interference, e.g. jammer, is well observable

  → Can be used for pattern optimization and/or direction of arrival (DOA) estimation of jammer

ADAPTIVE ARRAY SIGNAL PROCESSING
PRE-CORRELATION TECHNIQUES (2)

- Power minimization (PM) for null-steering in the direction of jammers

$$\boldsymbol{w}_{opt} = \arg\min_{\boldsymbol{w}} E\{|y|^2\} = \arg\min_{\boldsymbol{w}} \boldsymbol{w}^H \boldsymbol{R}_{xx} \boldsymbol{w} \ \text{subject to } w_1 = 1$$

The output power after weighting shall be minimized based on the constraint, that the weight for the signal of antenna element 1 w_1 is equal to 1.

- Up to N-1 nulls can be formed in the antenna reception pattern of an N element antenna array (one degree of freedom is consumed in the constraint for the reference element)
- GNSS satellite signals with the same direction of arrival as the jammer may also be nulled.

ADAPTIVE ARRAY SIGNAL PROCESSING
PRE-CORRELATION TECHNIQUES (3)

- Linearly constrained minimum variance (LCMV) beamformer

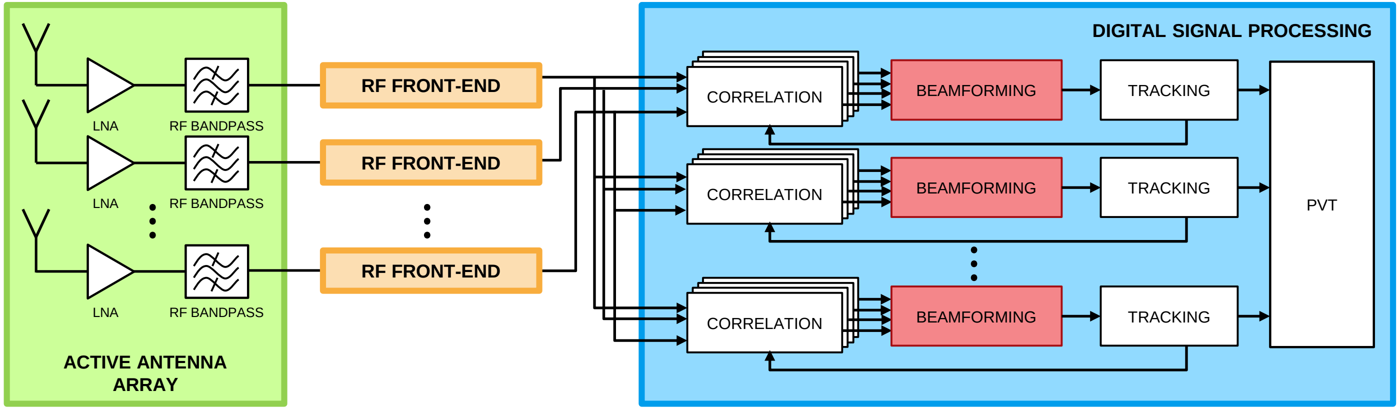
$$\boldsymbol{w}_{opt} = \arg\min_{\boldsymbol{w}} E\{|y|^2\} = \arg\min_{\boldsymbol{w}} \boldsymbol{w}^H \boldsymbol{R}_{xx} \boldsymbol{w} \ \text{ subject to } \boldsymbol{w}^H \boldsymbol{a}(r_j) = 1, j = 1, \dots, J$$

The output power after weighting shall be minimized based on the constraint, that the gain in the look directions ($\boldsymbol{a}(r_j)$) of J GNSS satellites is equal to 1.

– Requires knowledge of GNSS satellite positions (ephemeris) and receiver attitude (e.g. IMU data)
– Up to N-J nulls can be formed in the antenna reception pattern of an N element antenna array
– Reception of GNSS satellite signals may be improved compaired to plain power minimization

ADAPTIVE ARRAY SIGNAL PROCESSING
POST-CORRELATION TECHNIQUES (1)

- Typical architecture:



- After correlation, GNSS signals are well above noise floor
- Weight computation is performed on data after dispreading
- Individual set of weights for each receive channel

ADAPTIVE ARRAY SIGNAL PROCESSING
POST-CORRELATION TECHNIQUES (2)

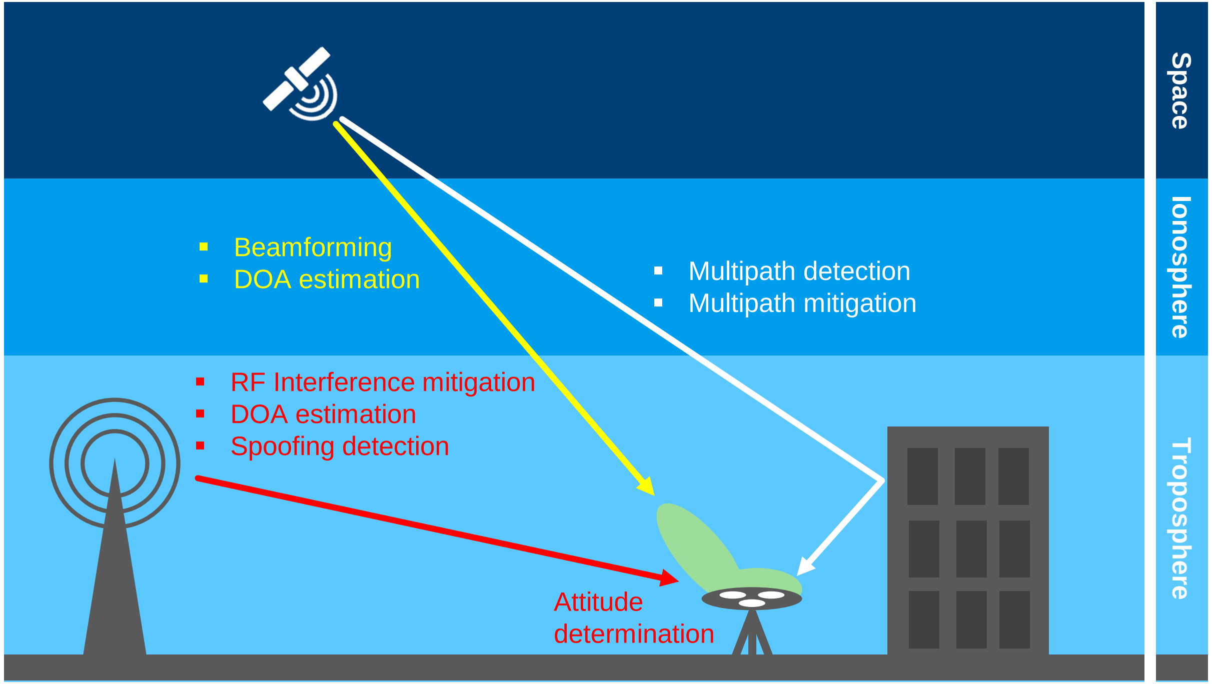
► Minimum Mean Squared Error (MMSE) beamforming

$$\boldsymbol{w}_{opt} = \arg\min_{\boldsymbol{w}} E\{|r - y|^2\} = \arg\min_{\boldsymbol{w}} E\{|r - \boldsymbol{w}^H \boldsymbol{x}|^2\}$$

The mean squared error of the receive signal with regards to the reference signal r, e.g. the local code replica, shall be minimized.

- A separate beam can be formed for each SV in view
- Susceptible to multipath induced errors

ADAPTIVE ANTENNA ARRAYS
BENEFITS



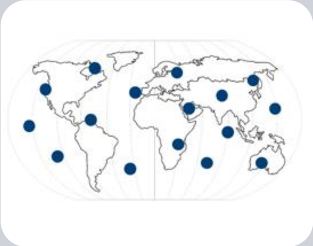
CONTENTS

GNSS THREATS AND MITIGATION TECHNIQUES

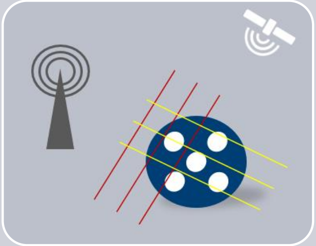
ADAPTIVE ARRAY PROCESSING TECHNIQUES

TEST SOLUTIONS FOR ADAPTIVE ANTENNA ARRAYS

TEST REQUIREMENTS FOR ADAPTIVE ANTENNA ARRAYS

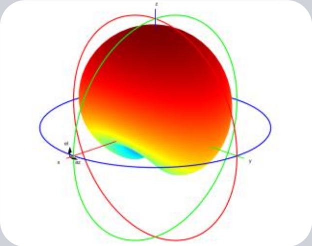


Multi-frequency multi-constellation support



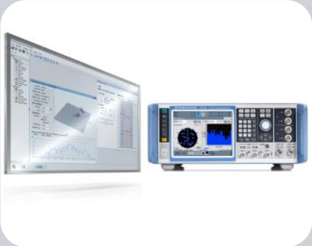
Precise amplitude, time and carrier phase alignment for

- Interfering signals
- Spoofing signals
- GNSS signals



Consider user-defined gain and phase antenna patterns

Scalability of test setup



Simulation of

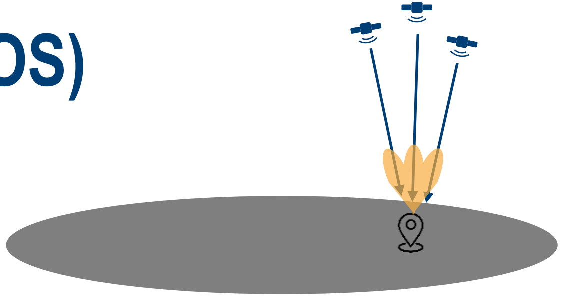
- RF interference with high J/S ratio
- Simulation of spoofing scenarios

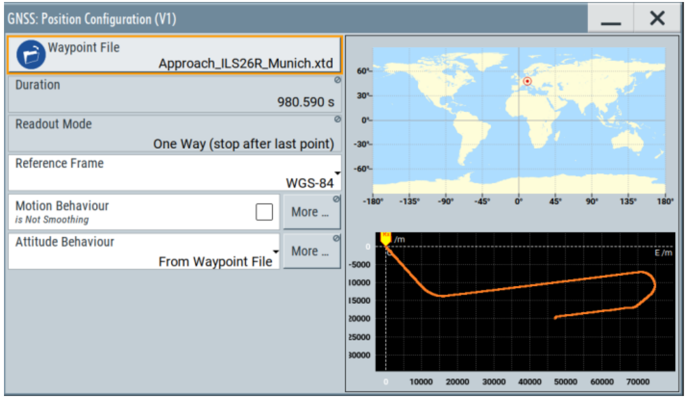
Intuitive scenario generation (manually and automated)

TEST SYSTEM FOR MULTI-ANTENNA GNSS RECEIVERS

- ✓ Based on the R&S®SMW200A Vector Signal Generator (VSG)
- ✓ Number of GNSS constellation simulators is scalable according to number of antenna array elements (here up to 8 antennas)
- ✓ Automated alignment in terms of amplitude, phase and time between individual RF outputs at a user-defined reference plane with R&S®RFPAL software
- ✓ Modular concept: subsets of simulators can be independently used
- ✓ Straight-forward configuration of complex jamming scenarios with the R&S®Pulse Sequencer software
- ✓ For interferer simulation with highest J/S ratio a separate RF output per antenna element is recommended

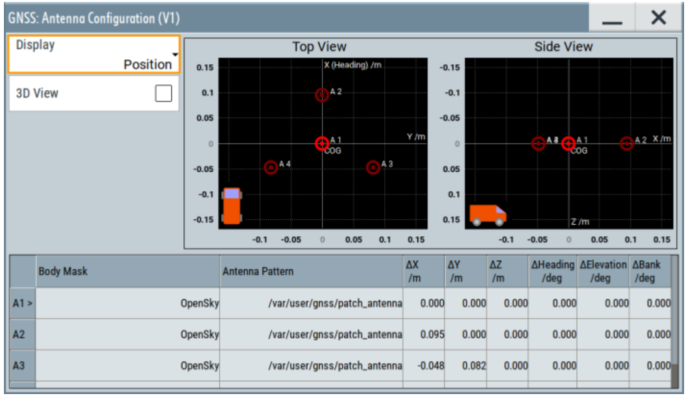
TEST CASE 1 – GNSS ONLY SIMULATION (LOS)

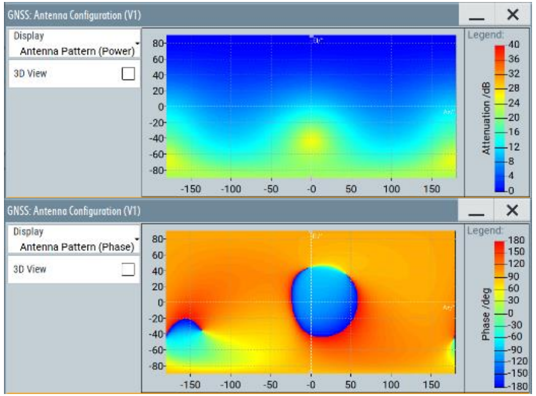




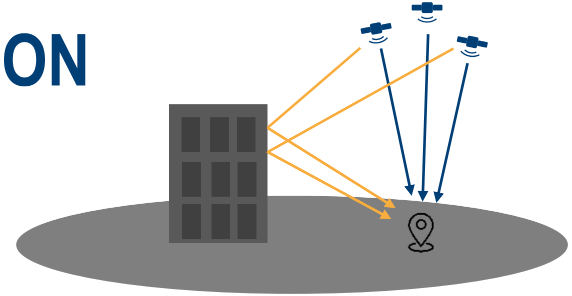
Applications:

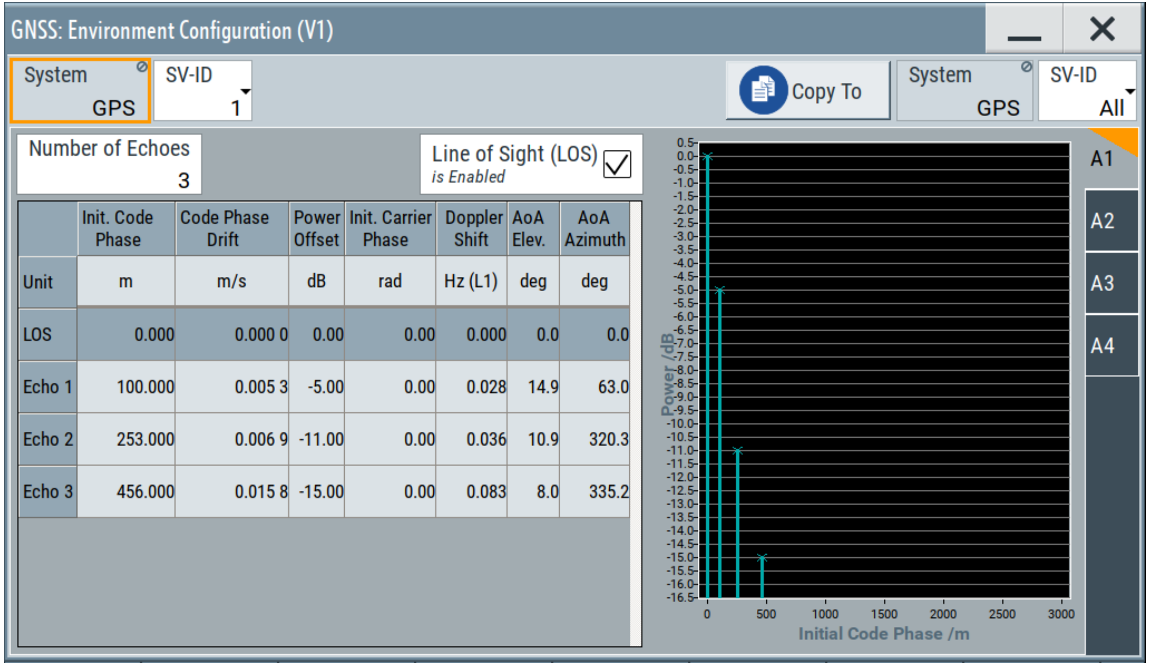
- Evaluation of beamforming algorithms
- Attitude determination
- Reference measurements





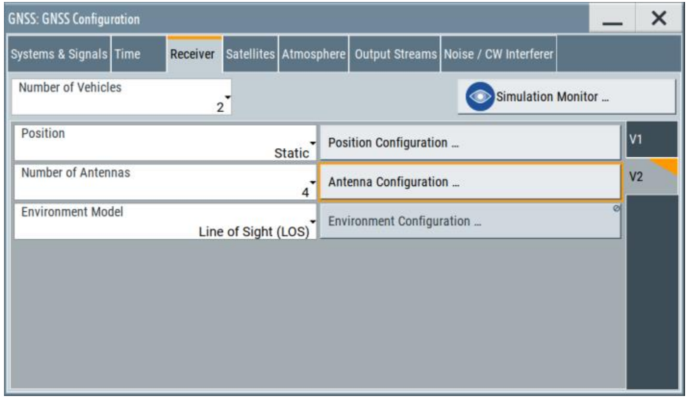
TEST CASE 2 – GNSS MULTIPATH SIMULATION



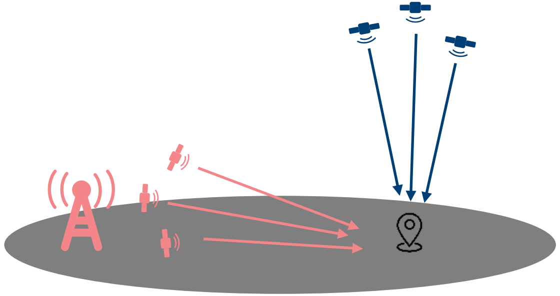


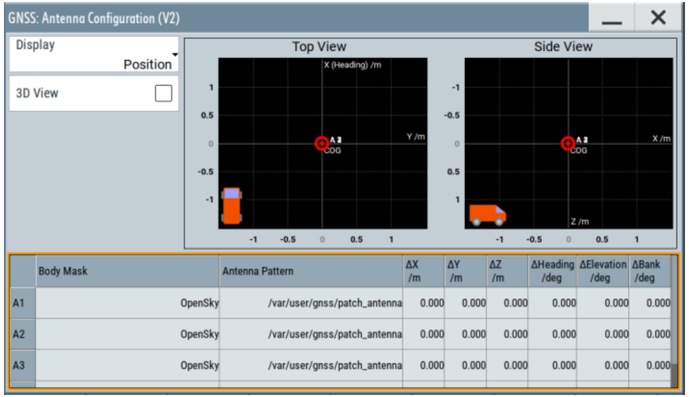
- Individual setting
  - Per SV
  - Per Antenna
- Up to 9 echoes per SV

TEST CASE 3 – SPOOFING SCENARIO



Second Vehicle

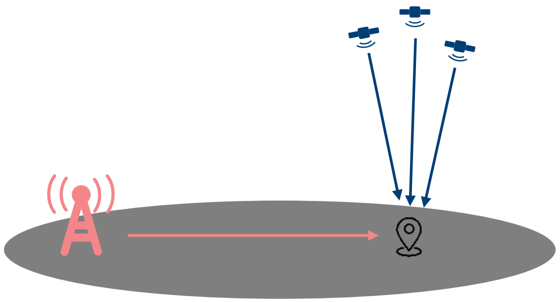




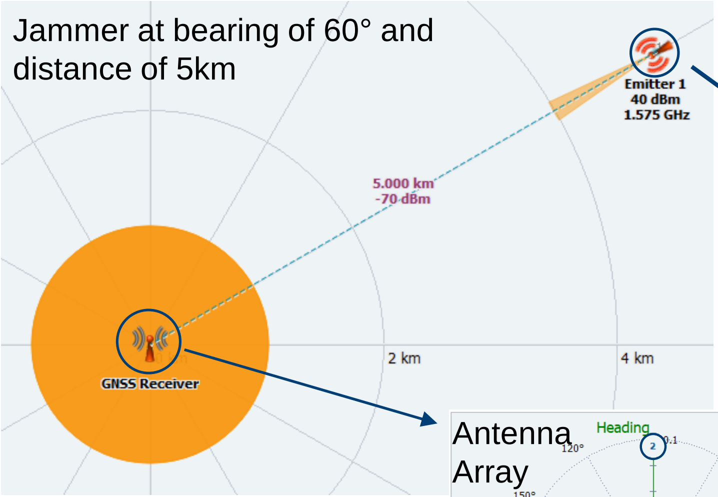
All antennas at same location

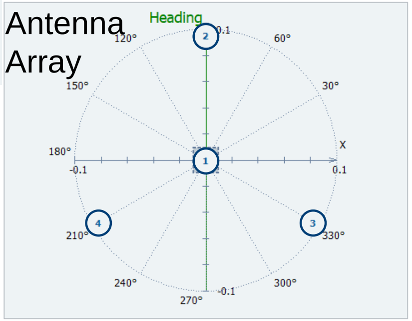
TEST CASE 4 – JAMMING SCENARIO

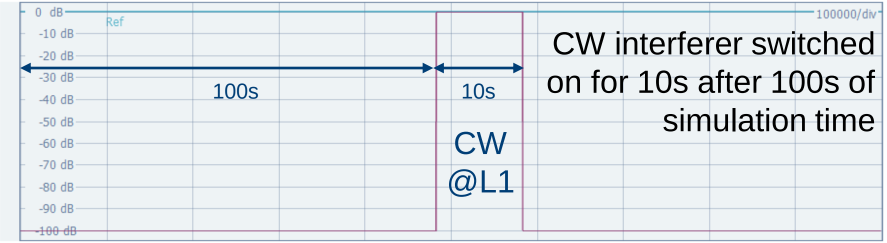
with R&S®Pulse Sequencer



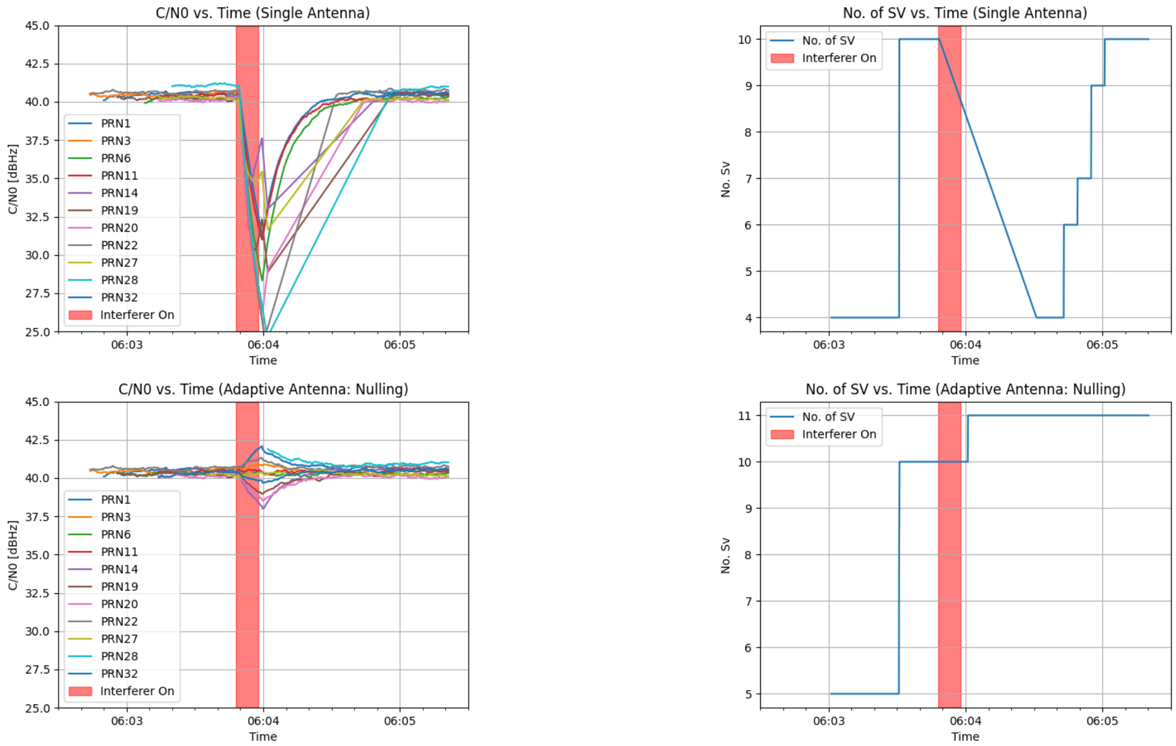
Jammer at bearing of 60° and distance of 5km







EXAMPLE TEST RESULTS – JAMMING SCENARIO



SUMMARY

Your task	Our solution	Your benefit
Simulation of unintentional interference		Scalable and modular concept
Simulation of multipath propagation		Automated amplitude, time and phase alignment
Simulation of jamming attacks		Integrated simulation of multipath and spoofing scenarios
Simulation of spoofing attacks		Straight-forward configuration of complex jamming scenarios

Find out more

www.rohde-schwarz.com/gnss

ROHDE&SCHWARZ

Make ideas real

EXAMPLE TEST RESULTS – JAMMING SCENARIO