Development of Array Receivers with Anti-Jamming and Anti-Spoofing Capabilities with Help of Multi-Antenna GNSS Signal Simulators

Andriy Konovaltsev, *German Aerospace Center (DLR)*
Emilio Pérez Marcos, Manuel Cuntz, Michael Meurer, *German Aerospace Center (DLR) and RWTH Aachen University, Germany*
Ronald Wong, Guy Buesnel, *Spirent Communications, UK*
Werner Lange, *Lange-Electronic GmbH, Germany*

BIOGRAPHIES

Andriy Konovaltsev received his engineer diploma and the Ph.D. degree in electrical engineering from Kharkov State Technical University of Radio Electronics, Ukraine in 1993 and 1996, respectively. He joined the Institute of Communications and Navigation of DLR in 2001. His main research interest is in application of antenna array signal processing for improving performance of satellite navigation systems in challenging signal environments.

Emilio Pérez Marcos studied Electrical Engineering at Valladolid University, Spain. From 2006 to 2008 he was granted a young research position within the Electronics Department at the same university. From 2009 to 2014 he worked as Research Engineer in the Medical Technology Industry in Jena, Germany. Since 2014 he has been working within the Algorithms and End-Devices group in the Institute of Communications and Navigation at DLR Oberpfaffenhofen. His current research topics include signal disturbances, interferences and cybersecurity in real time GNSS receivers and Spatial-Temporal Adaptive Processing techniques for multi-antenna systems.

Manuel Cuntz received the diploma in electrical engineering degree in 2005 from the Technical University of Kaiserslautern. He joined the Institute of Communications and Navigation of DLR Oberpfaffenhofen, in June 2006. His fields of research are multi-antenna satellite navigation receivers.

Michael Meurer received the diploma in electrical engineering and the Ph.D. degree from the University of Kaiserslautern, Germany. After graduation, he joined the Research Group for Radio Communications at the Technical University of Kaiserslautern, Germany, as a senior key researcher, where he was involved in various international and national projects in the field of communications and navigation both as project coordinator and as technical contributor. From 2003 till 2013, Dr. Meurer was active as a senior lecturer and Associate Professor (PD) at the same university. Since 2006 Dr. Meurer is with the German Aerospace Centre (DLR), Institute of Communications and Navigation, where he is the director of the Department of Navigation and of the center of excellence for satellite navigation. In addition, since 2013 he is a professor of electrical engineering and director of the Chair of Navigation at the RWTH Aachen University. His current research interests include GNSS signals, GNSS receivers, interference and spoofing mitigation and navigation for safety-critical applications.

Ronald Wong (BEng(1st Hons), MSc by Research(Distinction), PhD, CEng(RIN), MRIN) Ron received the BEng in RF Electronics from University of Surrey. He further pursued his interest by doing an MSc by Research and PhD in Satellite Engineering at Surrey Space Center, a research institute within University of Surrey. He was awarded the Chartered Engineer by Royal Institute of Navigation. Ron is employed by Spirent Communications as a Senior Systems Engineer. His research interest is in Global Navigation Satellite System and sensors fusion navigation.

Guy Buesnel (BSc(Hons), MSc(Eng), CPhys, FRIN) Awarded MSc (Eng) in Communications Engineering from the University of Birmingham, BSc (Hons) in Physics with Atmospheric Physics from the University of Wales Aberytstwyth. Guy is a Chartered

Physicist, a Member of the Institute of Physics and a Fellow of the Royal Institute of Navigation. Guy is employed by Spirent Communications as PNT Security Technologist, Robust Position, Navigation and Timing and his research interest is in Positioning Navigation and Timing Systems cyber-security.

Werner R. Lange is founder and President of Lange-Electronic GmbH, founded in 1977 in a western suburb of Munich. His main field of expertise covers a wide area from very precise time and frequency, real time clocks, GNSS systems, GNSS simulation tools and telemetry/data acquisition systems. He regularly presents papers at international conferences like PTTI, ITC, and ION in the USA, ETC and EFTF in Europe and many other conferences. Besides this he is member of the board of several technical and scientific organisations like EST (European Society of Telemetry) and PTTI (Precise Time & Time Interval) and works in different standardisation bodies.

ABSTRACT

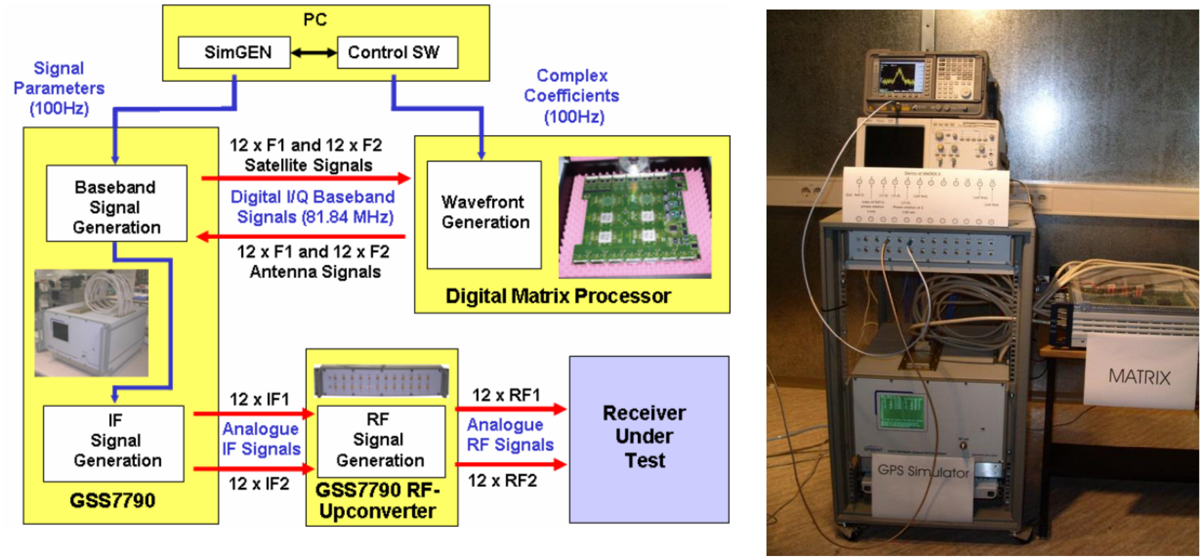
The paper focuses on the use of GNSS constellation simulators for the performance evaluation of advanced anti-jamming and anti-spoofing techniques of GNSS receivers using multiple antennas in an antenna array. The use of antenna arrays and array signal processing enables a GNSS receiver to apply extremely efficient countermeasures to counteract radio frequency interference. This enhanced resilience to jamming and spoofing makes the multi-antenna GNSS receivers very attractive in the context of safety-critical applications. The paper highlights the advantages of testing such receivers in a controlled laboratory environment by utilizing the multi-antenna GNSS simulators. A fully scalable architecture of the multi-antenna simulator based on the use of multiple simulator units is presented. The simulator composed of 8 single RF output simulators is used together with a GNSS multi-antenna receiver prototype (GALANT) developed by DLR in order to obtain exemplary results for beamforming, direction of arrival estimation and spoofing detection in the corresponding signal scenarios. The obtained results are also used to highlight the merits of a GNSS array receiver as part of promising anti-jam and anti-spoof solutions.

INTRODUCTION

Positioning and timing services provided by global satellite navigation system (GNSS) are likely to be strongly affected by signal distortions occurring in the radio propagation channel between a GNSS satellite and the user equipment. One type of such distortion is the radio frequency interference. Due to the low received GNSS signal power, it can be easily jammed intentionally or unintentionally. In addition, due to the open source nature of the navigation signal structure, it opens the door for spoofing attacks. The development of anti-jam and anti-spoof technologies in civilian domain, especially for those having safety aspects, is a hot topic of research ever since the time when the first GNSSs have started to deliver their services.

For more than twenty years the German Aerospace Center (DLR) conducts research in resilient GNSS receivers for safety-critical applications, focusing especially on the use of array signal processing techniques. In the past years, during the course of the development of a demonstrator of the resilient array receiver, DLR has gained a large experience in designing the entire signal processing chain. Different antenna and front-end setups as well as interference mitigation techniques in the time, frequency and space domain have been developed and analyzed. This development has been strongly relying on the use of the appropriate simulated GNSS signal, allowing for the extensive tests of the developed anti-jam and anti-spoof techniques in a fully-controlled and repeatable environment. In order to enable such simulations, an approach based on the utilization of a wavefront matrix was proposed in 2006, with the use of a modified Radio Frequency Constellation Simulator (see [1] for more details).

The wavefront matrix, an additional device developed by DLR (see Figure 1), was operating on the satellite signals in digital baseband of a modified multi-output GPS/Galileo Spirent Simulator GSS7790. The simulation of signals propagated to the antenna array aperture was performed by using a simplified narrowband assumption where the carrier phases were shifted according to the angle of arrival of each GNSS satellite. The baseband signals sampled at high rate were transferred in real time from the simulator to the wavefront matrix and back. As a result, the realization of the wavefront matrix approach required a dedicated external device and modified simulator hardware, high-speed and well-calibrated data transmission links.



a) block diagram b) practical realization

Figure 1 Approach to multi-antenna simulation by using wavefront matrix [1]

This paper describes a new generation multi-antenna simulator system that was developed to allow simulations of antenna array systems without the need for a unique modified hardware. In order to avoid the complexity of the use of the old system, this solution is based on the fully scalable architecture composed of multiple simulator units. To support all currently used arrays of GALANT demonstrator, the new and improved set-up utilizes 8 single RF output simulators with the capability to simulate antenna arrays with up to 8 elements. The simplification due to the narrowband assumption is no longer required since the complete signal modulation is now fed to the array aperture, which is very interesting for testing broadband techniques like, for example, Space Time Adaptive Processing (STAP). A high-power ground transmitter feature of the simulator allows for scenarios with interference-to-signal ratios of 100 dB and above. This feature enables for physical testing of anti-jam array-based techniques which was typically only possible with significant efforts in a very limited number of dedicated test environments.

The paper will give an overview of the architecture of the multi-antenna simulator along with the advantages associated with its use. The authors present test results for beamforming, direction of arrival estimation and spoofing detection capability of the DLR GNSS multi-antenna receiver prototype (GALANT). The presented results will highlight the advantages of testing using multi-antenna simulators and the merits of the DLR GNSS multi-antenna receiver prototype as part of a promising anti-jam and anti-spoof solution.

The rest of the paper is organized as follows. First, an overview of the architecture of the multi-antenna simulation system will be given. Next, the measurement set-up used in the laboratory trials is described. The next three sections will present the adopted simulation scenarios and the obtained results for (i) the jamming mitigation by using spatial nulling, (ii) the angle of arrival estimation for the received GNSS signals, and (iii) the joint array attitude estimation and spoofing detection. The paper ends with conclusions and an outlook to future developments.

MULTI-ANTENNA GNSS CONSTELLATION SIMULATOR

The complete system for multi-antenna GNSS constellation simulations based on Spirent GSS9000 series simulators is shown in Figure 2. It consists of one Main Host PC, two Auxiliary Host PCs, two Timing Masters (TM1 and TM2) and eight identical single antenna chassis signal generators (Aux 1 to Aux 8). The system makes use of a Distributed Engine architecture for the realization of a multi-output signal simulation. For this system, one Auxiliary Host PC controls four signal generators, whereas each of the two Auxiliary Host PCs is, in turn, managed from the Main Host PC where the Spirent proprietary simulation software, SimGEN, is running. Timing Masters act as a timing reference to synchronize individual antenna chassis of the signal generators. Each signal generator is capable to simulate up to six GNSS constellations and two constellations of Ground Transmitters (GTx) serving as embedded interference sources. The supported GNSS constellations are GPS L1/L2/L5, GLONASS L1/L2, Galileo E1/E5/E6, BeiDou B1i/B2i and QZSS L1. A Ground Transmitter enables to simulate an interference signal of different types like continuous wave (CW), broadband noise, matched spectrum PRN-code modulation, pulsed modulation etc. Such a signal can be allocated to any frequency band of a supported GNSS constellation.

Figure 2 Spirent CRPA Simulation System

The simulator can be configured to work in the following configurations:

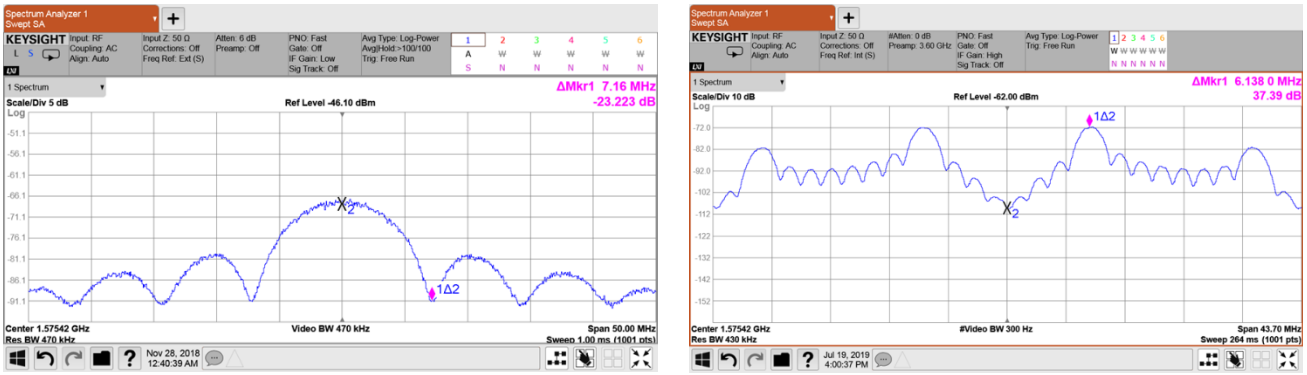
1. "8 Outputs Mode": Simulation of up to eight receiving antennas. In this configuration the system is made up of the Main Host PC controlling Auxiliary Host PCs 1 and 2, Timing Master 1, signal generators Aux1 to Aux 8.
2. "4+4 Outputs Mode": The system is divided into two independent simulator, each capable of simulating of up to four receiving antennas. In this configuration the first simulator is made up of Auxiliary Host PC 1, Timing Master 1 and signal generators Aux 1 to Aux 4. The second simulator is built of Auxiliary Host PC 2, Timing Master 1 and signal generators Aux 5 to Aux 8.
3. "Flexibility Signals": The generation of non-standard GNSS signals by using only Auxiliary Host PC 1, Timing Master 1 and Data Server. In this configuration Timing Master 1 acts as a signal generator. This novel simulator feature is described in more details below.

Non-Standard GNSS Signal Generation

This novel feature allows user to define alternative, non-standard GNSS signal modulation and navigation message content – so called flexibility signals. The flexibility signals can be simulated on the following GNSS constellation frequencies: GPS L1/L2/L5, Galileo E1/E5/E6 and BeiDou B1i/B2i. Each signal channel of the Flexibility Signal Generator generates two signal components, where each of the components can be defined with its own by the following parameters:

1. PRN sequence and chipping rate
2. Binary Offset Carrier or Linear Offset Carrier modulation
3. Navigation message content and data rate
4. Assignment to the ±I or ±Q phase
5. Frequency sweeping
6. Signal pulsing

Two examples of the spectra of flexible signals generated at GPS L1 carrier frequency are shown in Figure 3.



a) BPSK(7) modulation b) BOC$_{cos}$(6, 1.5) modulation

Figure 3 Spectra of simulated flexibility signals

CRPA Antenna Calibration Signal

Another novel feature of the developed simulation system is the availability of a special reference signal for calibrating carrier phase alignment between individual antenna channels of a CRPA receiver. Its purpose is to calibrate off carrier phase changes in the analog and digital parts of the signal path after the CPRA antenna elements on the fly, e.g. due to temperature drift or cables' movement. Therefore when the system is configured in the "8-outputs" and "4+4 Outputs" setups, the calibration signal can be added to the simulation to be present at all times for each carrier frequency used by the simulated GNSS constellations. For example, when simulating GPS L1 and Galileo E1 constellations, the calibration signal will only be generated at 1.57542 GHz. With GPS L1 and GPS L5, two calibration signals at L1 and L5 carrier frequencies will be generated. The calibration signal is constellation specific, e.g. BPSK(1)-modulated for GPS L1, BOC(1,1) for Galileo E1, so that is can be acquired and tracked in a very similar way as the corresponding standard GNSS signals. The user can define the PRN number, power level and center frequency offset of the signal. The calibration signal is not modulated by a navigation data stream.

Other distinctive features of the developed simulation system are:

- The Distributed Engine architecture used to connect the Main Host PC to the two Auxiliary Host PCs, controlling eight signal generators, simulating of up to six frequency bands per signal generators at a time at the update rate of the parameters of the produced RF signals of 1000 Hz.
- The code phase alignment of the calibration signal for up to six frequency bands is maintained to pico-seconds range with respect to the 1PPS signal across all eight signal generators throughout the course of simulation.
- The carrier phase alignment of the simulated GNSS signals is maintained to within 2 degrees for all six frequency bands, across all eight signal generators, throughout the course of CRPA system simulation.

The next section will present the measurement set-up used to obtain illustrative results for beamforming, direction of arrival estimation and spoofing detection with the help of the new multi-antenna GNSS constellation simulator and an experimental GNSS array receiver.

MEASUREMENT SET-UP

The receiver used for the laboratory tests is a four inputs DLR's GALANT receiver [2]. The receiver makes use of several array signal processing techniques for increasing the resilience against jamming and spoofing phenomena: pre-correlation spatial nulling of the strong interference signals, post-correlation beamforming for enhancing the signals of interest (i.e. navigation signals from the GNSS satellites), direction of arrival estimation and spoofing detection operating on the estimated directions. The receiver can be directly connected to four RF ports of the Spirent CRPA Simulation System as shown in Figure 4. The simulator is fully configurable in SimGEN control software (see Figure 5). In order to simulate the CRPA antenna configuration, the simulation scenario adopts a user receiver with four antennas. The positions of the four receiving antennas, i.e. the positions of their carrier phase reference points, are set to represent the actual array hardware (see Figure 6). The gain and phase reception patterns of the simulated array elements can be additionally used for making the simulation of the antenna array reception more realistic.

The figures of merit used to assess the performance of the array GNSS receiver can be obtained with the help of the graphical user interface (GUI) of GALANT (see Figure 7). The following observations are used further in the paper to assess the receiver performance: carrier-to-noise density ratios (C/N0s) of the tracked navigation signals, estimated directions of arrival (DOAs) of the signals, estimated array attitude and the spoofing detection metric derived from DOAs. GALANT GUI also allows to save the data obtained from the receiver in a log file for later analysis of the performance metrics. This feature is used to compute and plot the time evolution of such metrics as the mean number of tracked satellites and mean C/N0s.

Figure 4 DLR's GALANT receiver connected to Spirent CRPA Simulation System

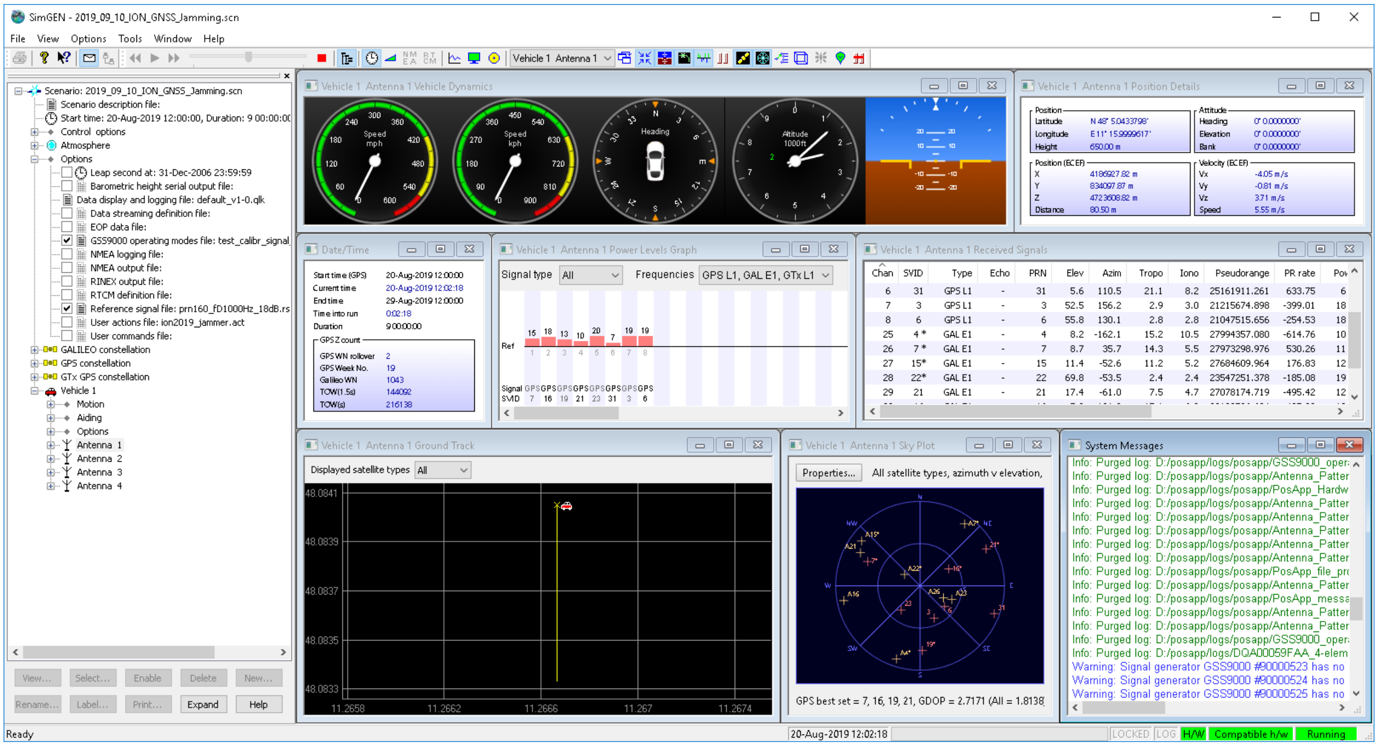
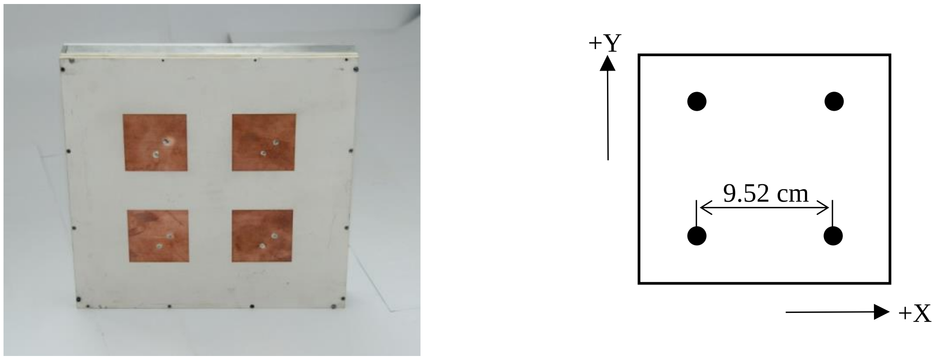


Figure 5 Spirent SimGEN control software



a) DLR's L1/L5 2-by-2 antenna array b) antenna positions used by simulator

Figure 6 Antenna array of GALANT receiver and its model used by Spirent simulator

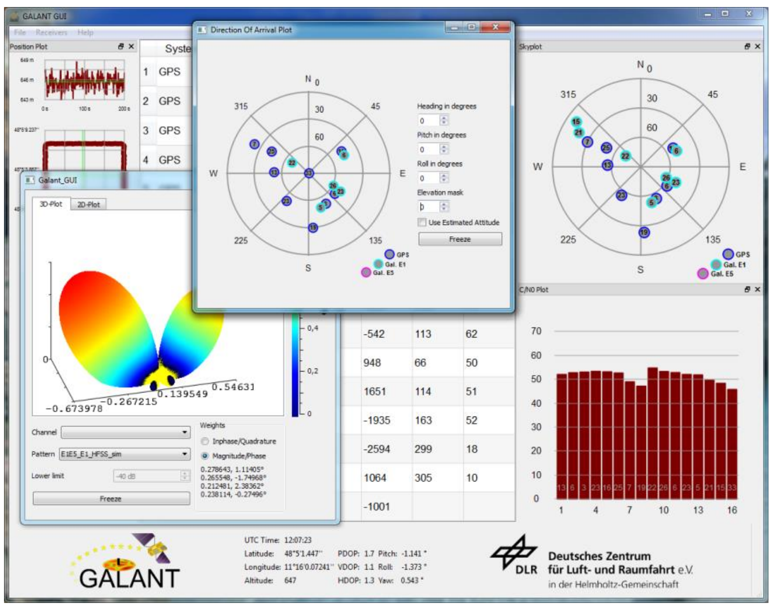


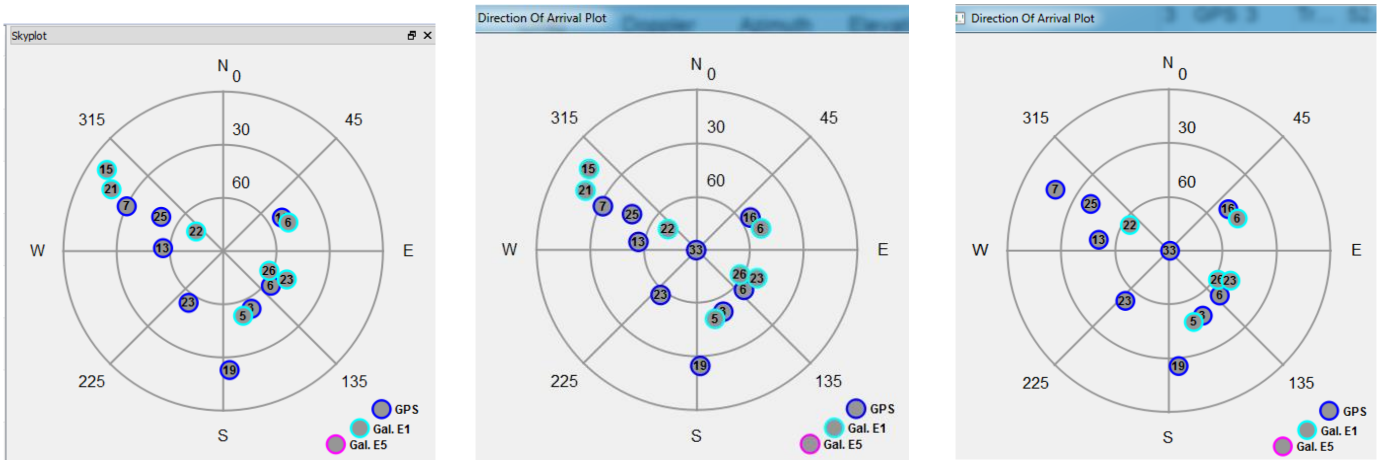
Figure 7 Graphical user interface of GALANT receiver

The next sections will demonstrate how the multi-antenna simulation system introduced above can be used to test in controlled laboratory conditions the operation of the GNSS array receiver in interference-free, jamming and spoofing scenarios.

INTERFERENCE-FREE SCENARIO

Testing under interference-free conditions is required to validate the nominal receiver performance. With an array receiver being the unit under test, additional receiver functions need to be tested such as beamforming and direction of arrival estimation. The corresponding test results are shown in the figures below. The simulation was divided in two parts. In the first part the user was assumed to stay at a fixed position for 5 minutes, while in the second part the user was moving along a quadratic track (see Figure 12) which resulted in 90-degree turns of the heading of the user platform.

Figure 8 presents the estimated directions of arrival for GPS and Galileo satellites at some time during the first static part of the simulations. The results in Figure 8b have been obtained in the simulation run where the gain and phase patterns of the individual antennas were simply adopted as isotropic. It can be observed that at such conditions the estimated DOAs come very close to the true directions computed by using the satellite ephemerides (see Figure 8a). The SimGEN software allows to integrate the actual gain and phase reception patterns of the user antennas on the corresponding GNSS carrier frequency into the simulation. This feature of the simulator was used to assess the effect of realistic antenna characteristics (see Figure 9) on the DOA estimation process. The corresponding results are presented in Figure 8c. As can be observed from this figure, the DOA estimation is no longer available for some satellites signals arriving to the antenna array from low elevation angles. Also it can be observed, that the estimated directions of arrival for other satellites do not match the true ones so well as in case of the array elements being simulated as isotropic. The presented illustrative results show how the DOA estimation function of the array receiver can be first tested under simplified idealistic assumptions in order to identify possible implementation issues and then under more realistic conditions allowing to assess the expected performance in the field.

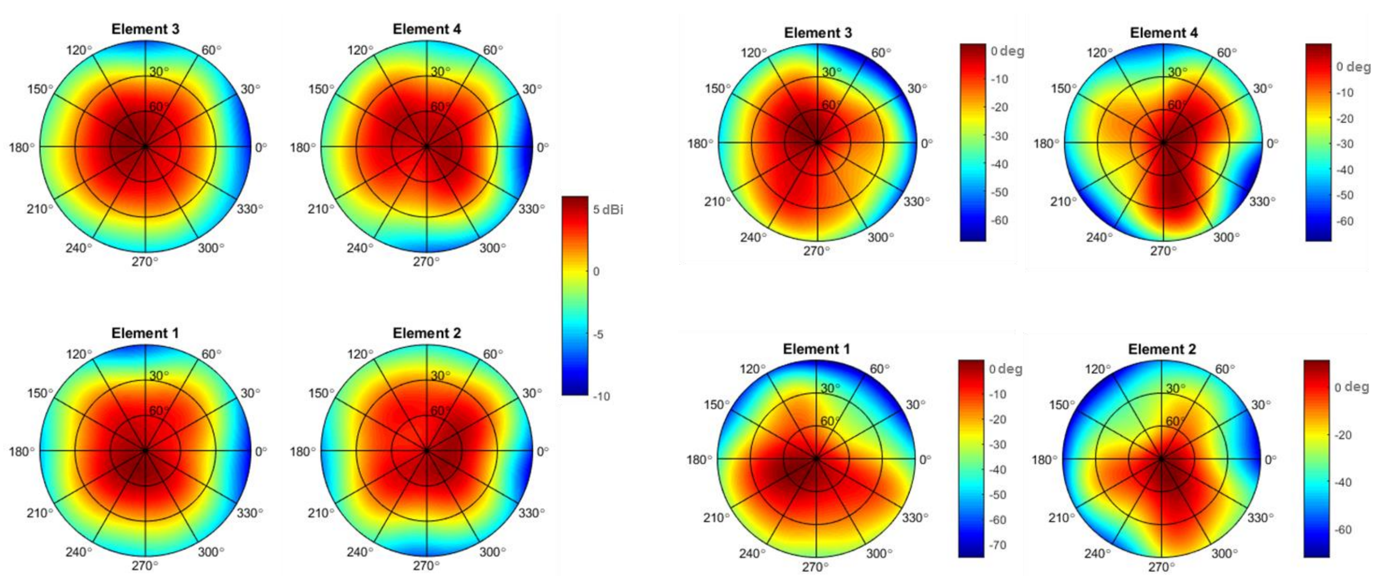


a) true DOAs

b) simulation adopting isotropic array elements

c) simulation using realistic gain and phase patterns of array elements

Figure 8 Estimated directions of arrival for a static receiver

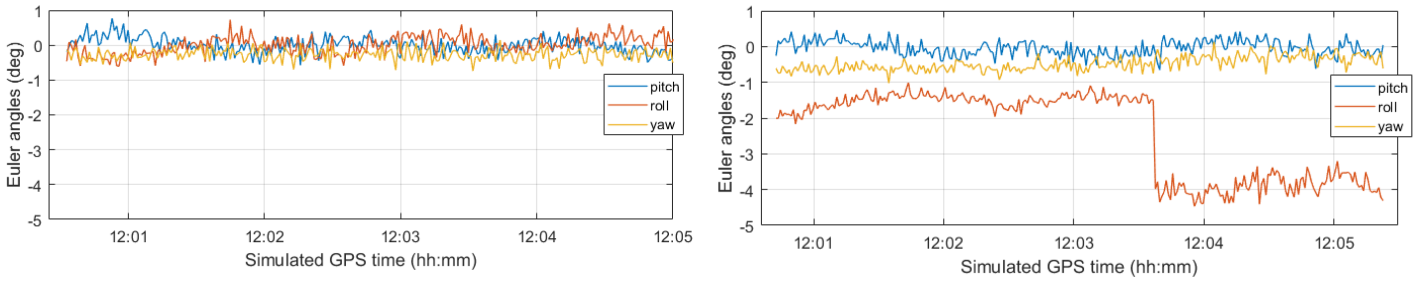


a) gain patterns

b) phase reception patterns

Figure 9 Realistic gain and phase patterns of array elements used in simulations

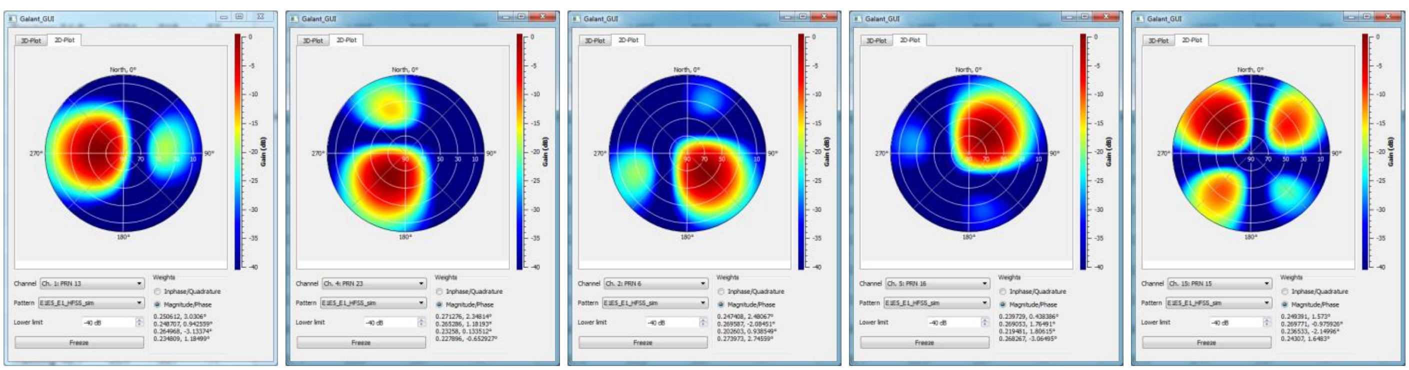
Figure 8 shows that an array GNSS receiver performing DOA estimation can provide two types of the information about the directions to the GNSS satellites: (i) true directions of arrival in a global coordinate system and (ii) the DOA estimates in the local coordinates of the antenna array. These types of information can be used to estimate the attitude of the antenna array [3]. The corresponding results obtained in the first static part of the test can be seen in Figure 10. It can be observed how the biases in DOA estimations in the case of using realistic radiation patterns of the array elements propagate into the biases in estimated Euler angles. Especially it can be seen how the availability of a strongly biased DOA estimation for Galileo PRN 21 starting from simulation time 12:03:35 produces stronger bias in the estimation of the roll angle (see Figure 10b).



a) simulation adopting isotropic array elements b) simulation using realistic patterns of array elements

Figure 10 Estimation results for array attitude

The correct operation of the post-correlation beamforming can be verified by observing the generated reception patterns of the antenna array for different satellites. Such patterns, also often referred to as beam patterns, are computed as a weighted sum of the reception patterns of the array elements where the complex array weights are produced by the beamforming technique. Some of beam patterns reported by GALANT GUI during the static part of the test are shown in Figure 11. It can be observed that the beam pattern in a given tracking channel has an obvious high-gain area (indicated by dark red color in the plots in Figure 11) which is located around the direction of arrival of the corresponding GNSS signal (compare with DOAs in Figure 8a).



a) GPS, PRN 13 b) GPS, PRN 23 c) GPS, PRN 6 d) GPS, PRN 16 e) Galileo, PRN 15

Figure 11 Beam patterns generated by GALANT receiver in different satellite tracking channels

Figure 13 presents the estimated directions of arrival during the second part of the simulation where the user starts to move along a quadratic track (see Figure 12). The rotation of the estimated DOAs that corresponds to the change of the heading of the user platform at different sides of the quadratic track can be observed. The change of the orientation of the antenna array in a simulation scenario allows analyzing the dynamic performance of the beamforming and DOA estimation processes.

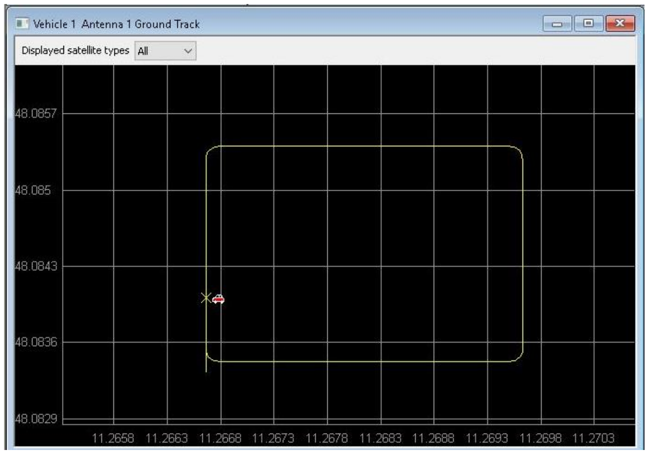
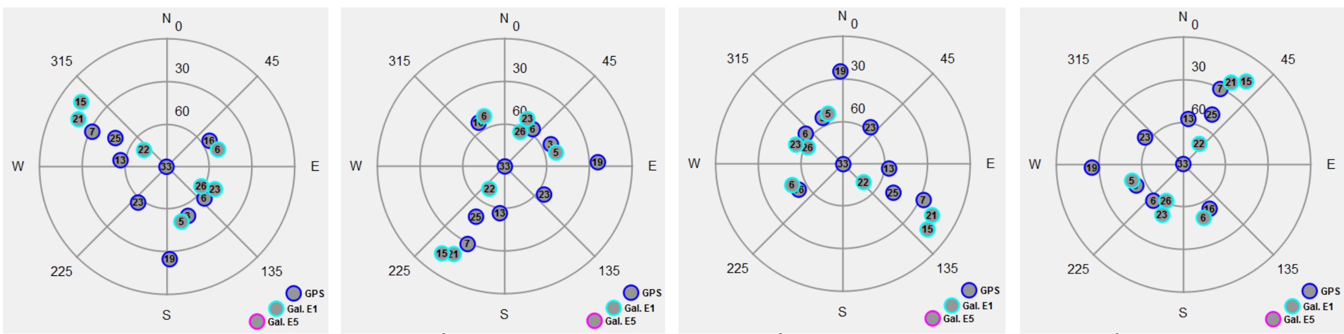


Figure 12 Simulated user motion track



a) at 1st segment of track b) at 2nd segment of track c) at 3rd segment of track d) at 4th segment of track

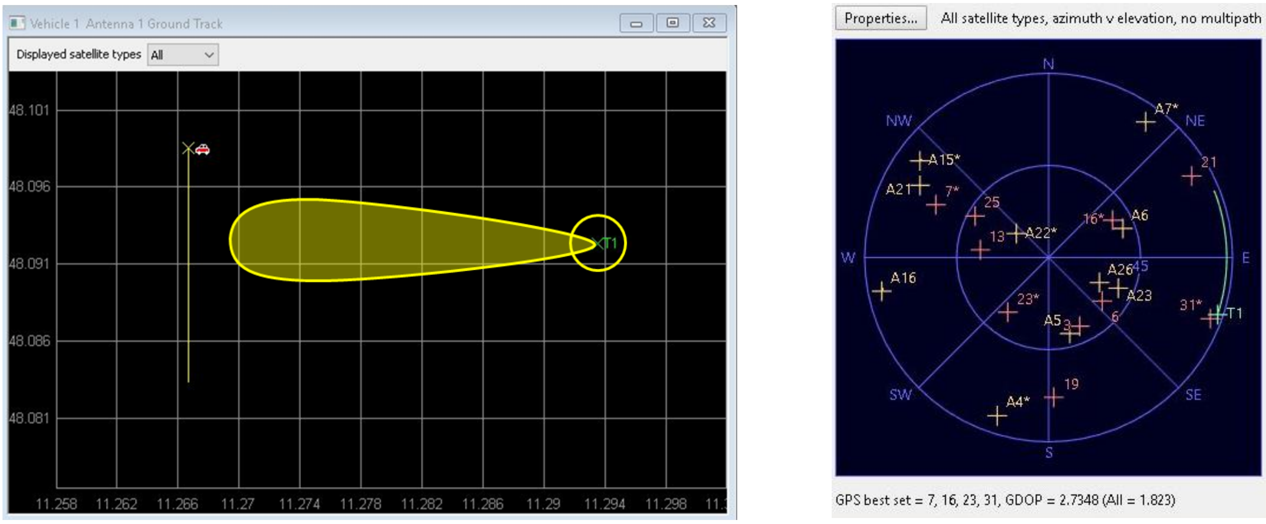
Figure 13 Estimated directions of arrival for the user following the rectangular track

JAMMING SCENARIO

Testing of the array GNSS receiver in a jamming scenario can be easily realized by using the Ground Transmitter (GTx) option of the Spirent simulation system. This option allows integrating in a simulation scenario up to 16 in-band interference transmitters for each GNSS band. Each of the signal generators Aux1 - Aux8 is capable to produce dedicated interference signals with power levels up to -23 dBm. Several interferer types are available including the continuous wave, BPSK modulation, continuous wave pulse, AWGN, FM, AM and phase modulation signals. Similar to satellite signals, each interferer is simulated with the power level, code- and carrier-phases which exactly correspond to the distance between the GTx and the antenna position. For an array receiver, e.g. CRPA system, with multiple receiving antennas this results in realistic simulation of the spatial properties of the interference signals and allows for testing anti-jamming techniques based on array signal processing. This testing approach can be considered as a valid alternative or at least as a valuable preparation step prior to field tests, e.g. such as those described in [4] or [5].

The simulation scenario used for testing anti-jamming performance of the GALANT receiver follows the testing approach of the jamming field trials performed by DLR in Galileo Testbed (GATE) in Berchtesgaden, Germany in 2011 [5]. The user vehicle moving with the speed of 55 km/h is exposed to radio frequency interference as it passes an interferer source located in the vicinity of the road (see Figure 14). In order to simulated shadowing of the interference signal that can, for example, occur in urban canyons, the radiation antenna of the jamming source is adopted to be strongly directive.

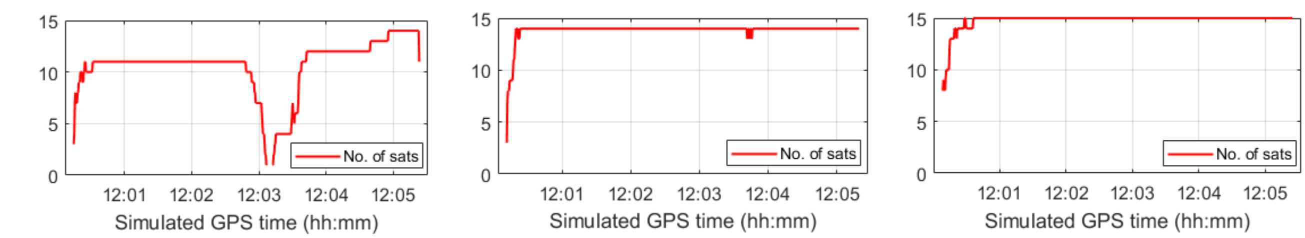
The test results obtained with the different configurations of the GALANT receiver are presented in Figure 15 and Figure 16. The test metrics used to assess the resilience of the receiver to jamming are the mean carrier-to-noise density ratio (C/N0) that is averaged over all satellites being in track and the number of the satellite being tracked.



a) motion track of user vehicle, radiation pattern and location of jammer b) DOA of jammer in skyplot (T1, in green)

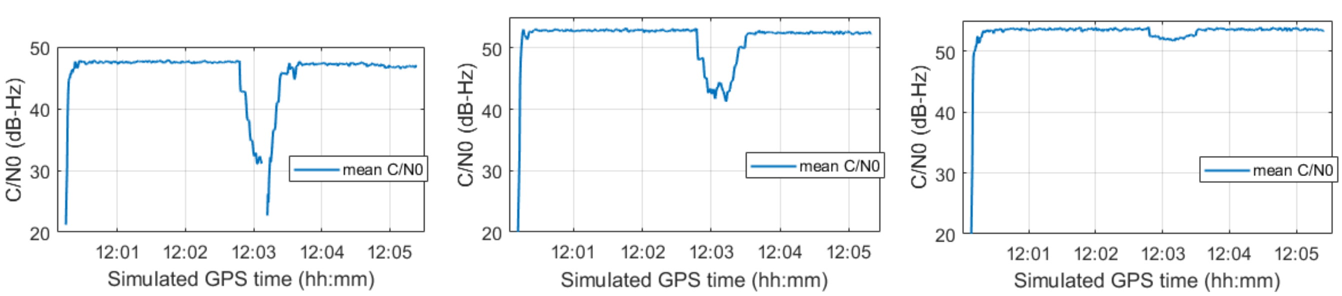
Figure 14 Realization of jamming scenario

By observing the plots for the test metrics in Figure 15 and Figure 16 it can be concluded that the use of adaptive antenna array technology enables to significantly increase the resilience of the receiver. The smallest jamming effect is observed if both adaptive pre-correlation nulling and post-correlation beamforming are utilized. But even the use of adaptive beamforming at the post-correlation stage of signal processing, i.e. in the baseband software of the receiver at low sampling rate and therefore with a small additionally required computational load, can bring significant improvement.



a) single-antenna reception b) array reception, post-correlation beamforming c) array reception, pre-correlation spatial nulling and post-correlation beamforming

Figure 15 Number of satellites in track



a) single-antenna reception b) array reception, post-correlation beamforming c) array reception, pre-correlation spatial nulling and post-correlation beamforming

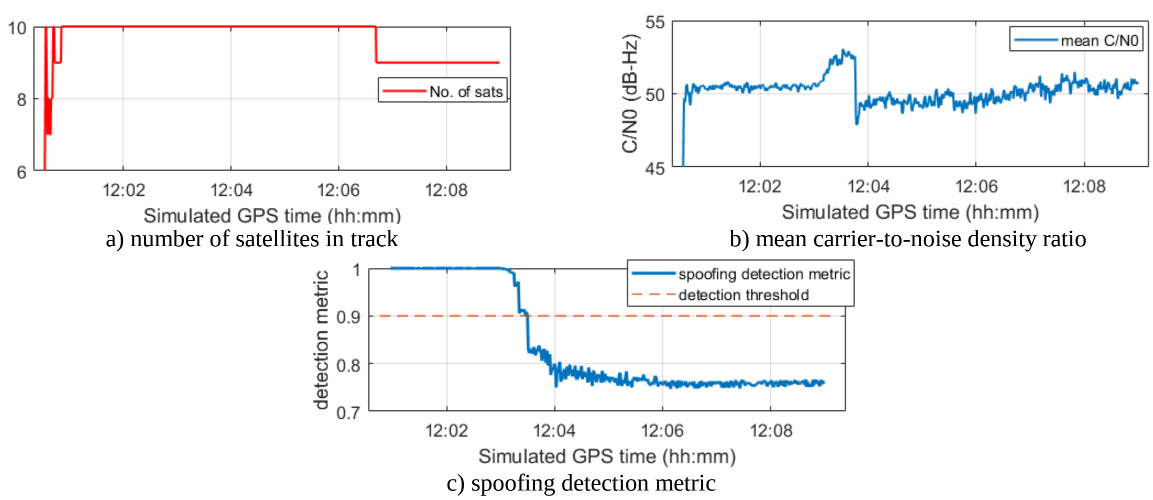
Figure 16 Mean carrier-to-noise density ratio

SPOOFING SCENARIO

The spoofing scenario used for the tests in this section is similar to the Case 4 "Static matched power, position push" of the Texas Spoofing Test Battery (TEXBAT) introduced in [6]. Two users, one corresponding to authentic signals and another one corresponding to the spoofing signals, are simulated. The output of an individual signal generator, e.g. Aux 1, is in this scenario a mixture of two simulated antenna outputs of both users. This is possible due to the special option "two vehicles – single RF output" of the simulator: the signals simulated for the same antenna index of both users (e.g. output of antenna 1 of the first user and output of antenna 1 of the second user) are summed up together in the simulator hardware. At the start of simulation both users share the same static position. During the first three minutes of simulation the signals of the second user are switched off. After that, the signals of the second user start to rise step-by-step in power until they become 2 dB stronger than the corresponding signals of the first user. As next, the second user starts to move northwards with the speed of 5 km/h. This type of spoofing attack can be classified as "S7 - Targeted Sophisticated Spoofer" according to the nomenclature proposed by U.S.-EU Working Group C in [7]. Such spoofers can potentially use multiple phase-synchronized transmit stations in order to overcome the receiver defense strategies based on multiple receiving antennas and exploitation of the spatial properties of incoming signals. Although such types of spoofing attacks can be also simulated with the Spirent CRPA solution, a simple scenario with a single spoofing transmitter station is adopted in this paper for obtaining illustrative results.

In order to simulate a single direction of arrival for all signals received by the second user, the following approach is used. The antennas of the second user are not arranged in a 2-by-2 array but placed into the geometric center of the antenna array of the first user. The phase patterns of the antennas of the second user are set to be isotropic with the phase relations between the elements corresponding to a single direction of arrival.

The results of the test are presented in Figure 17, Figure 18 and Figure 19. The time evolution of the mean C/N0 and the number of tracked satellites in Figure 17 clearly indicate that the spoofing attack was successful. The phase where the tracking loops of the receiver are taken over by more powerful spoofing signals can be identified between simulation times 12:03 and 12:08. In this time both the authentic and spoofing signals fall into the code-delay aperture of the code tracking loops and the evolution of the C/N0 metric reflects the changes in the superposition of the signals from constructive at the beginning the spoofing attack (where C/N0 grows) to predominantly destructive (C/N0 falls below the level before the attack). The spoofing detection metric (see Figure 17c) obtained as a result of the joint attitude estimation and spoofing detection process [8] enables to reliably detect the spoofing attack after a short time. This is due to the fact that the estimated directions of arrival reflect the presence of the spoofing signals and start to strongly deviate from the non-distorted DOA estimations shown in Figure 18a. When the tracking loops are pulled sufficiently far away from the code-delay-positions of the authentic signals, the estimated DOAs converge to a single point corresponding to the direction to the spoofing source as shown in Figure 18b. The similar behavior can be also observed for the post-correlation beamforming where the beam patterns produced in different satellite tracking channels show the high-gain area around the same direction (see Figure 19).

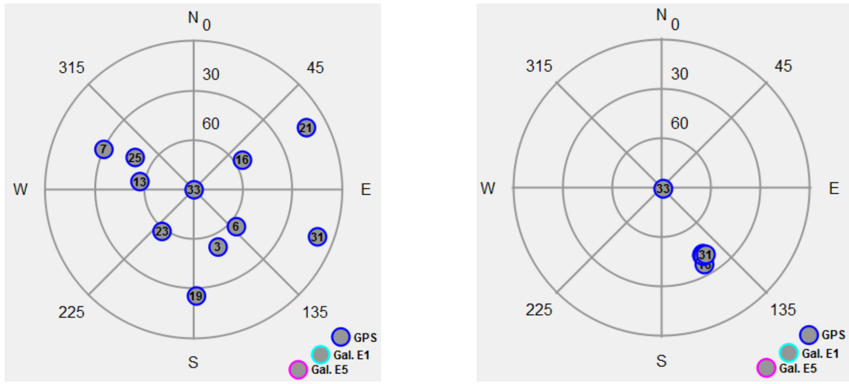


a) number of satellites in track

b) mean carrier-to-noise density ratio

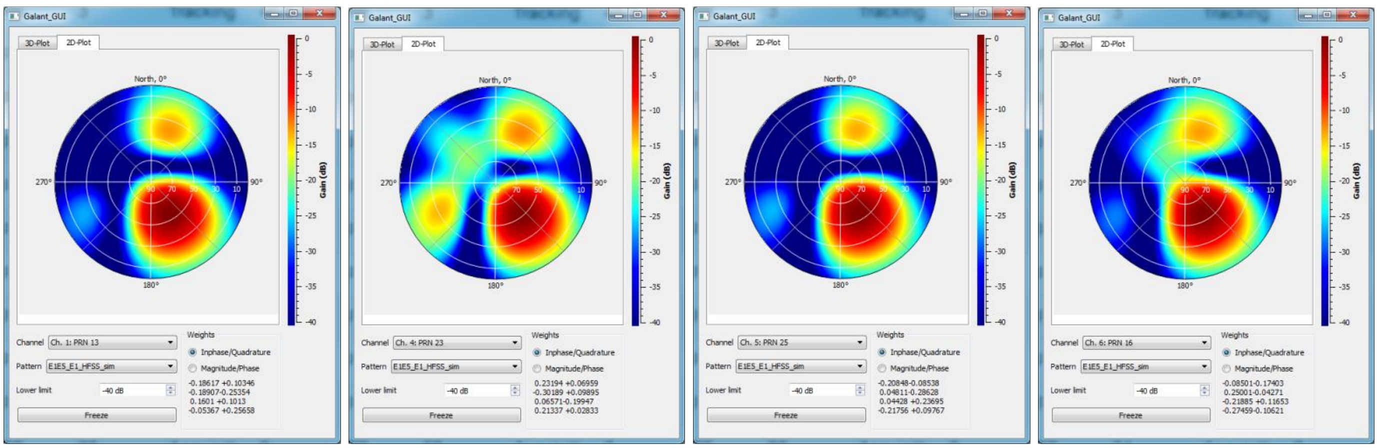
c) spoofing detection metric

Figure 17 Test metrics in spoofing attack simulation



a) before spoofing attack (12:02) b) at the end of spoofing attack (12:08)

Figure 18 Direction of arrival estimation in spoofing attack simulation



a) Ch. 1: GPS, PRN 13 b) Ch. 4: GPS, PRN 23 c) Ch. 5: GPS, PRN 25 d) Ch. 6: GPS, PRN 16

Figure 19 Beam patterns produced in different satellite tracking channels at the end of spoofing attack (12:08)

CONCLUSIONS

Some illustrative results of testing a GNSS receiver utilizing an adaptive antenna array technology for counteracting jamming and spoofing attacks have been presented. The test results clearly show that the development process of GNSS receivers with adaptive antenna arrays can greatly benefit from the use of new generation of multi-antenna GNSS constellation simulators. This new generation of simulators, e.g. Spirent CRPA solution introduced in the paper, is characterized by:

- Easy scalability with respect to the number of antennas as well as the number of GNSS constellations to be simulated;
- Exact carrier phase alignment between individual antenna outputs;
- Integrated simulation of radio frequency interference;
- Large choice of options to simulate spoofing scenarios;
- Possibility of integrating gain and phase patterns of user antennas into the simulation;
- Availability of flexible signals simulation to support the development of navigation signals of new generation of GNSS.

All these features allow efficient testing the functionalities of the array GNSS receivers under controlled laboratory conditions, speeding up the development process and reducing to a large extent the need for costly and time consuming field test. This approach is already used by DLR to develop anti-jamming and anti-spoofing solutions for safety-critical applications of GNSS.

REFERENCES

[1] Hornbostel, A., Denks, H., and Venus, H., "First Results of Baseband Wavefront Generation with a Digital Channel Matrix for Testing of CRPA," *Proceedings of the 19th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2006),* Fort Worth, TX, USA, September 2006, pp. 780-789.

[2] Heckler, M. V. T., Cuntz, M., Konovaltsev, A., Greda, L. A., Dreher, A., and Meurer, M., "Development of Robust Safety-of-Life Navigation Receivers," *IEEE Trans. Microw. Theory Tech.*, vol. 59, no. 4, pp. 998–1005, Apr. 2011.

[3] Meurer, M., Konovaltsev, A., Cuntz, M., and Hättich, C., "Robust joint multi-antenna spoofing detection and attitude estimation using direction assisted multiple hypotheses RAIM," *Proceedings of the 25th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2012)*, Nashville, TN, September 2012, pp. 3007-3016.

[4] Cuntz, M., *et al.*, "Field Test: Jamming the DLR Adaptive Antenna Receiver," *Proceedings of the 24th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2011)*, Portland, OR, September 2011, pp. 384-392.

[5] Cuntz, M., *et al.*, "Vector Tracking with a Multi Antenna GNSS Receiver," *Proceedings of the 25th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2012)*, Nashville, TN, September 2012, pp. 2050-2056.

[6] Humphreys, T. E., Bhatti, J. A., Shepard, D. P., and Wesson, K. D., "The Texas Spoofing Test Battery : Toward a Standard for Evaluating GPS Signal Authentication Techniques," *Proceedings of the 25th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2012)*, Nashville, TN, September 2012, pp. 3569–3583.

[7] Fernandez-Hernandez, I., *et al.*, "Increasing International Civil Aviation Resilience: A Proposal for Nomenclature, Categorization and Treatment of New Interference Threats," *Proceedings of the 2019 International Technical Meeting of The Institute of Navigation*, Reston, Virginia, January 2019, pp. 389-407.

[8] Appel, M., Konovaltsev, A., and Meurer, M., "Robust Spoofing Detection and Mitigation based on Direction of Arrival Estimation," *Proceedings of the 28th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2015)*, Tampa, Florida, September 2015, pp. 3335-3344.