Real World Direction of Arrival Estimation and Mitigation of Spoofing Signals with a Synthetic Aperture Antenna

J. Dampf[(1)], T. Pany[(1)], W. Bär[(2)], J. Winkel[(2)], C. Stöber[(2)], L. Mervart[(3)], J. A. Avila Rodriguez[(4)] , R. Ioannides[(4)]

[(1)] IGASPIN GmbH
Reininghausstraße 13a, 8020 Graz, Austria
Email: J.Dampf@igaspin.at

[(2)] IFEN GmbH
Alte Gruber Straße 6, 85586 Poing, Germany

[(3)] Department of Geomatics, Czech Technical University
Thákurova 7, 166 29 Praha 6, Czech Republic

[(4)] ESA/ESTEC
Keplerlaan 1, 2201 AZ Noordwijk, The Netherlands

INTRODUCTION

Nowadays 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 are intentional attacks on a GNSS receiver to mislead or degrade the navigation solution. Spoofing is considered as a serious thread, especially when spoofing GNSS reference stations distribute their degraded or falsified correction data to many GNSS users.

Whereas the position of a reference station (and its time) is typically well known and cannot be spoofed, a sophisticated spoofing attack may induce multipath like effects or ionospheric-like effects on the measured pseudoranges and carrier phases. This attack will degrade the performance of the reference station and the service relying on the reference station data. These spoofing signals don't need a high signal power and may be well below the line-of-sight signal power. They are thus very difficult to detect as standard methods like signal-quality-monitoring, C/N0 monitoring or a time series analysis still see the line-of-sight signal as main contribution. An efficient method, to detect those attacks is direction of arrival (DoA) estimation, which is discussed in this paper by making use of a synthetic antenna aperture and advanced detection and mitigation techniques.

The outline of the paper is as follows. In the first three sections the operation principle of a GNSS synthetic aperture antenna is summarized outlining how it can be used to detect and eliminate even weak spoofing signals. The fourth section contains results from a bit-true simulation of a static GNSS receiver (= conventional reference station) and of a synthetic aperture system both experiencing the same spoofing attack. The fifth section describes the real-world spoofing experiment conducted on a parking lot near the IFEN premises. The sixth section presents some results of the real-world spoofing results, demonstrating the ability of the spoofer to degrade the static station and the ability of the synthetic aperture antenna to detect and mitigate the spoofing attack. Finally an outlook is given.

All work has been performed within the Galileo Evolution Programme EGEP funded project SETI (no. EGEP-ID 89-1.11) of the European Space Agency (ESA).

BACKGROUND

A synthetic aperture GNSS antenna combines GNSS signals received at different spatial locations to optimize a certain performance criterion. Like phased array antennas, they allow to form a certain antenna gain pattern and can thus be used to eliminate the effect of spoofing signals [3]. Synthetic aperture antennas have so far received only limited attention from the GNSS community. Proof-of-concepts have been shown in [1]. The work in [2] did investigate several signal processing options for synthetic aperture antennas.

As in [1] we used in this work a rotating GNSS antenna. The antenna motion is measured precisely with a magnetic sensor allowing to determine the antenna position with sub-millimetre precision at every instant. The antenna rotates with a rate of 1 Hz and has a rotation radius of 50 cm. The rotation plane is horizontally aligned.

A rotating antenna is mechanically relatively easy to realize and all mechanical components can be chosen for long-term operation without any maintenance. A radio-frequency (RF) slip ring is needed to connect the GNSS antenna.

The key advantages of a synthetic aperture antenna over a phased array system are that it allows realizing larger apertures with less effort. Furthermore, electrical calibration is not needed as only a single antenna element is involved. Also, the (pre-correlation) receiver design is much simpler as only one RF signal needs to be processed. The disadvantages are that only signals with a known coherency can be processed and the mechanical movement is potentially prone to cause an increased overhead.

OPERATION PRINCIPLE OF A SYNTHETIC APERTURE ANTENNA

The basic operation principle of the chosen synthetic aperture system is shown in Fig. 1. It can be seen to be a variant of a vector tracking receiver. If the receiver has a position, velocity and time (PVT) solution available, the receiver predicts this solution for the next beamforming interval (of e.g. a duration of 1 s) and uses this prediction to compute replica signals. The replica signals are then correlated against the received GNSS signal from the rotating antenna. The correlation time interval is short (e.g. 4 ms) and in this case 250 correlation values are obtained for each received GNSS satellite signal.

The correlation values are collected for satellites and all code phase offsets (e.g. early, prompt and late). Then the impact of the satellite motion and the receiver clock drift and jitter is removed. Especially the receiver clock is a nontrivial impact on the correlation values and using more stable oscillators (e.g. OCXOs or atomic frequency standards) considerable simplifies the receiver clock estimation efforts.

Once those effects are removed, it can be shown that the correlation values can be treated in way as if they were received at the same instant. Consequently, the whole theory for phased array systems can be employed. If a GNSS receiver operates on a real antenna array, digital beamforming and null steering techniques can be employed, allowing an update of the array weight vector per the time-varying signals conditions, and thus adjusting the radiation pattern of the antenna array dynamically, at each instant. In contrast to the synthetic array approach considered in SETI, the signal collected at different spatial locations is available at the same time instant. Noise and the desired signal components from the different locations are correlated, even without any correlation with internal replicas being applied.

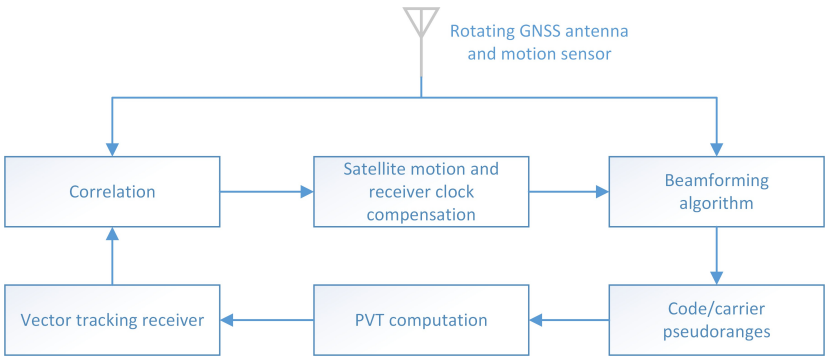

Fig. 1. Block diagram of synthetic aperture processing

There are basically two parts in the signal processing with antenna arrays, one is the beamforming that adapts the antenna radiation pattern to enhance the reception of the signals of interest and cancels the interferences as much as possible, and the other is the estimation of the direction-of-arrival of the signals and interferences.

There are two types of beamforming, data independent and statistically optimum. The first type of beamforming does not depend on the received signal but only on side information (e.g. direction of arrival of the signals and potential interferences are already known). The adaptability of such a beamformer is very limited, they can thus be used only when the context is very well known; else it would lead to poor performance.

The second type of beamforming (i.e., statistically optimum), uses the received signal to determine the weight vector and the antenna radiation pattern. Such beamformer can thus adapt to the changing environment, e.g. when a new interference appears. This type of beamforming performs an optimization process to determine the weight vector. It can be a maximization process, such as the maximization of the signal-to-noise ratio, or of the signal-to-interference-and-noise ratio; or it can be a minimization process, such as the minimization of an error between a model and the actual signals (Minimum Mean Square Error (MMSE) algorithm), or of the variance of

the beamformer output (Linearly Constrained Minimum Variance (LCMV) algorithm, or Minimum Variance Distortion-less Response (MVDR) algorithm). A disadvantage of the MMSE algorithm is that it requires the generation of an accurate reference signal (training sequence) at the receiver; also, it does not impose constraints on the solution (i.e. the weights). On the contrary, the LCMV and MVDR algorithms include constraints in the optimization process and thus constraints in the response of the beamformer, such that a certain gain in the direction of the signal of interest can be guaranteed.

The beamforming algorithm produces combined correlation values eventually exploiting the spatial diversity. Those correlation values form then the basis for the generated code and carrier pseudoranges. It is of importance to consider distortion-less response algorithms, as they ensure that the beamforming does not introduce any biases in the code or carrier pseudoranges.

SELECTED BEAMFORMING

Within the SETI project an adaptive beamforming algorithm was selected, as shown in Fig. 2, tailored to handle spoofing signals. Being more an engineering solution, it first eliminates the line-of-sight signals from the compensated correlation values by applying suitable Null operators. This can be done to high precision, as the DoA of the line-of-sight signals is known. In the next step, the received signal power is estimated as a function of the DoA. This is done on a grid of elevation and azimuth values with a grid resolution of 1 deg. It should be noted, that the raw beam width of the synthetic aperture antenna is on the order of 10 deg, due to the selected diameter of 1 meter and a wavelength of 19.03 cm.

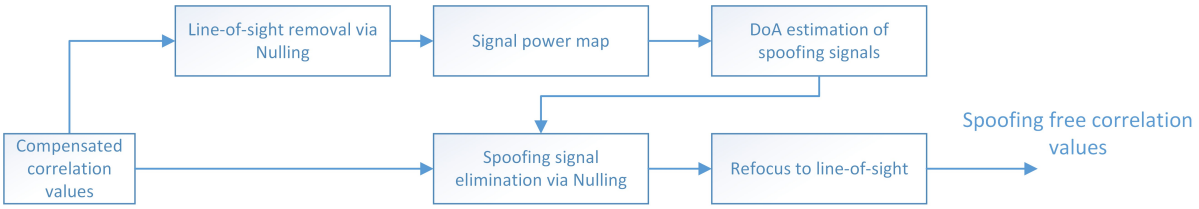

Fig. 2. Chosen beamforming algorithm with DoA estimation and Nulling

In case no spoofing signal is present (and no strong specular multipath reflection), the estimated received signal power is noise like. In case a spoofing signal is present, it clearly shows up as peak in this map (see later sections for real-world data) and its DoA can be retrieved.

The position of the peaks are used to identify the DoA of the spoofing signals, which itself is used to construct a Null operator to eliminate the spoofing signals from the compensated correlation values. After the spoofing signals have been eliminated, it is reasonable to assume that only the line-of-sight is present and by focusing the synthetic aperture antenna gain towards the line-of-sight optimal correlation values are obtained.

A characteristic of the chosen method is that spoofing signals are treated independently of their power. In other words, a weak spoofer is treated the same as a strong spoofer (provided the weak spoofer is detected). On contrast a MVDR beamformer will react more adaptively on varying signal strengths. Furthermore, the implemented algorithms all require either pilot signals or known navigation data bits. Estimation of unknown navigation data symbols (or bits) for the line-of-sight or for the spoofer signals is currently not considered.

SIMULATION RESULTS

Prior to conduction of real-world experimentation, a bit-true simulation of a spoofing attack on L1 and L2 has been performed. A static GNSS antenna was considered and a synthetic aperture antenna. A so-called multipath attack was assumed. The spoofing signal was 6 dB lower than the line-of-sight signal, and did use as spoofing position the true position, however artificially varying the line-of-sight ranges between +/- 30 m around the true value. By doing this rather large ranging errors are introduced to the station under attack.

For the simulation of the synthetic aperture antenna, only line-of-sight signal maximization is used (the Nulling algorithm was not yet ready at the time of doing the simulations). But already focusing the gain towards the line-of-sight significantly reduced the impact of a spoofing signal due to the beam width of around 10 deg.

The data was analysed with a GNSS data analysis software package called lmSoft, which was developed by the Prague Technical University and specifically adapted for our analysis purposes. In this case, we used it in a (simulated) precise-point-positioning (PPP) mode.

In Fig. 3 we see the PPP performance over a duration of 30 min. The convergence of the estimated coordinates to the true coordinates is given only for the synthetic aperture station. One may speculate that the static receiver may converge after several hours, but this has not been investigated. The synthetic aperture system converges quickly within a few minutes.

It should be noted that even for the synthetic aperture processing significant (code and carrier) residuals are present. This is a consequence of using only the line-of-sight maximization but not the Nulling of the spoofing signals.

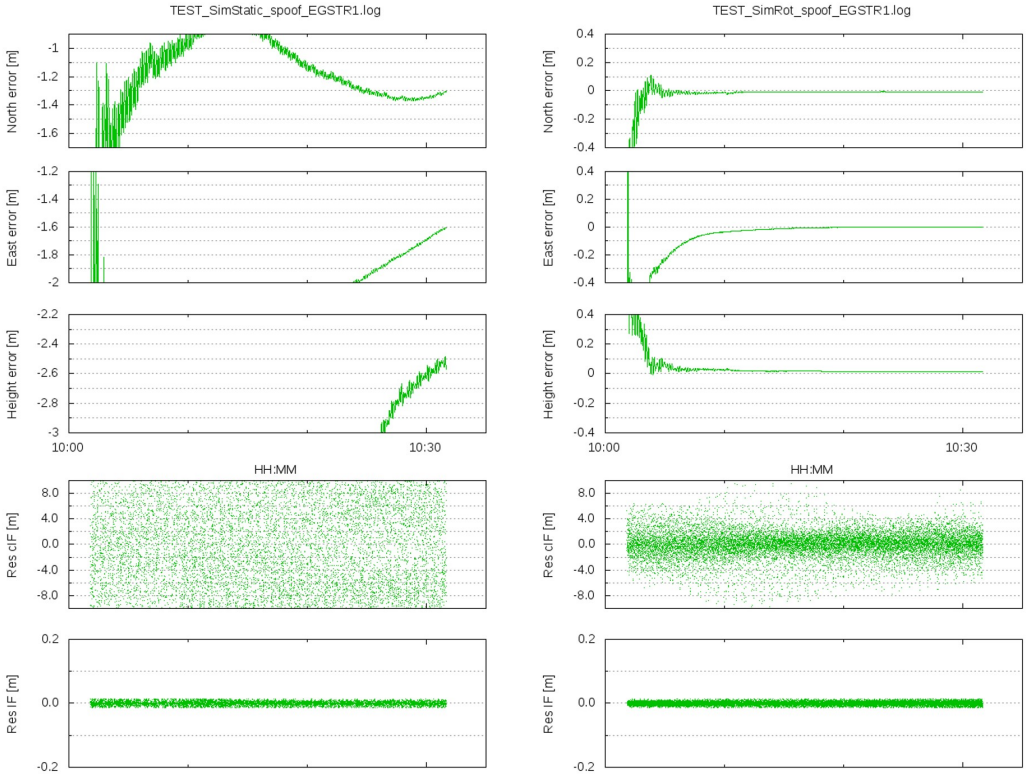

Fig. 3. Simulated PPP performance of GNSS station (left: static, right: synthetic aperture) under a spoofing multipath attack. All units are in meters, the fourth row are the GPS L1/L2 code pseudorange residuals for all satellites, the fifth row are the GPS L1/L2 carrier pseudoranges for all satellites.

REAL-WORLD SPOOFING TEST SETUP

The spoofing setup used within SETI for real-world tests consists of a NavX-NCS RF constellation simulator operated in a dedicated spoofing mode. The simulator is time synchronized to Signal-In-Space (SIS) via a rubidium atomic clock. Furthermore, an additional GNSS receiver delivers demodulated navigation data symbols. Those symbols are collected over a certain time and are then predicted to allow real-time transmission of the true symbols. The spoofing mode allows applying position/velocity and time/time drift offsets to the truth target PVT. Fig. 4 shows the principal setup.

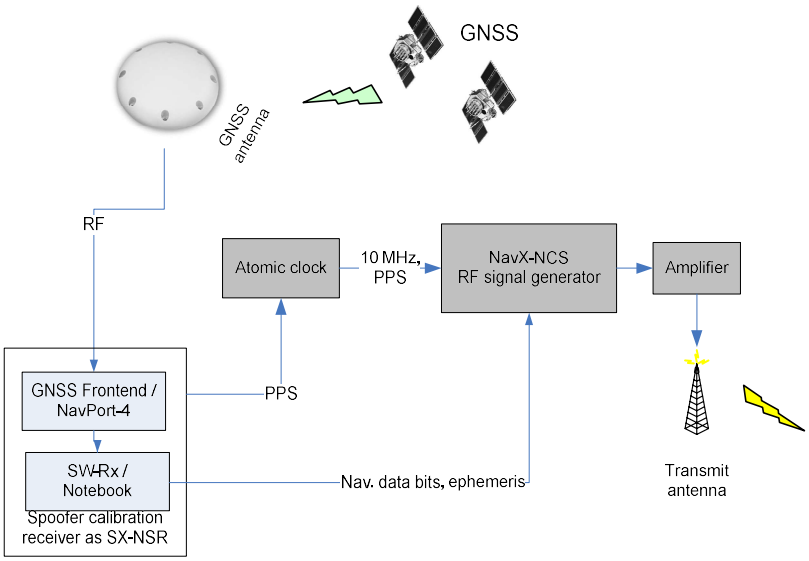

Fig. 4. Spoofing signal generation setup

The setup was installed in a 19“ rack in the laboratory with a 20 meter RF cable to the transmit antenna on the roof. The complete setup with all RF cables (SIS antenna to transmit antenna) was calibrated with a test receiver connected to the RF output of the signal simulator for the exact delay between the pulse-per-second (PPS) of the rubidium clock and the PPS of the test receiver receiving a spoofing signal. The determined offset was configured in the spoofing mode setup of the NavX-NCS simulator for compensation. To compensate the free space loss further 55 dB amplifiers were connected to the RF output to provide further margin in addition to the simulator internal amplifier.

The tests were performed at IFEN premises. The transmit antenna was installed on the roof pointing to the receivers under tests (one static and one rotating antenna receiver) placed on the parking desk. On the other side of the roof, outside the effects of the spoofing signal, a second static and rotating antenna receiver used as reference were installed and running throughout the experimentations. Figure 5 shows the setup with both views from and to the parking deck.

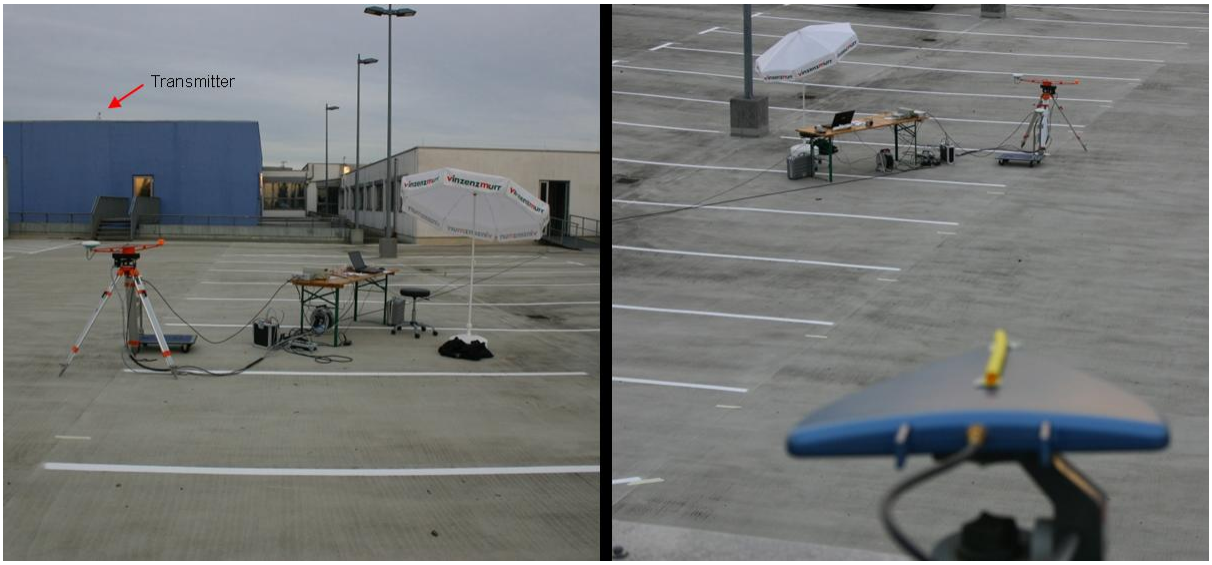

Fig. 5. Test area on the parking deck with view from the receiver under attack up to the transmitter on the roof (left) and from the transmit antenna down to the test receivers (right)

The setup was used in a several days test campaign to perform the following spoofing attacks:

- Multipath spoofing without any offset to the truth position and time.
- Position spoofing with introducing a velocity after initial multipath spoofing to take over the receiver.
- Time spoofing by introducing an increasing time drift after initial multipath spoofing to take over the receiver.

Furthermore, with an additional transmit antenna, the azimuth angular resolution of the spoofer detection was determined. The spoofing signal was splitted at RF level and transmitted over two transmit antennas with an angle of around 30 degree to the test receiver. While the first transmit antenna was kept static the other transmit antenna was gradually re-positioned and moved step by step nearer to the static first transmitter until they were both side by side.

INITIAL REAL-WORLD SPOOFING RESULTS

This section covers some results of the spoofing detection and mitigation experiments which have been performed on the parking deck of IFEN premises. The results show that a coherent spoofer with a bit true navigation message and synchronized GNSS time can be detected and mitigated with the previously discussed methods. The herein presented results refer to the position spoofing scenario, where the spoofer tries to take over the tracking loops of the receiver under attack and moves the position solution eastwards. Additionally, the effect of position spoofing is shown on a static receiver with typical FLL/PLL/DLL tracking and is compared to the results of the synthetic aperture antenna PVT results which applies spoofing detection and mitigation techniques. All spoofing experiments have been performed on L1 GPS C/A and Galileo E1 OS pilot. The herein presented scenario starts with open sky tracking of the true GNSS signal. After five minutes the spoofing attack is started and the falsified PVT solution coincides with the attacked receivers PVT solution to take over the tracking loops smoothly, which means that the correlation function of the spoofer is exactly located in the LOS signal correlation function. Figure 6 shows the multicorrelator output of the SX3 receiver during a spoofing attack with a constant position displacement of several hundred meters to the true PVT to verify that a spoofing signal is actually present, which results in a clearly separated correlation function in the code phase direction.

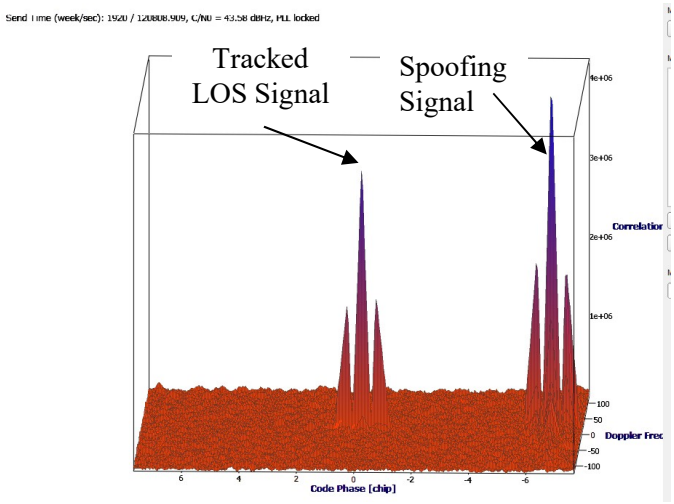

Fig. 6. Doppler-Delay map of a typical receiver under spoofing attack, showing Galileo E1 pilot; spoofed PVT with a constant position offset

Spoofing Detection and Mitigation: The above described beamforming method (spoofing detection and Nulling) allows to estimate the signal power coming from a spatial direction by projecting the received signal onto the expected phase signature and integration over the beamforming interval. Based on this, signal power maps spanned over azimuth and elevation can be derived, which are shown in Fig. 7. The upper plots show the received signal power with an adjustable greyscale in a typical satellite sky plot, while in this case +10 dB to LOS relates to black and -25 dB to LOS relates to white. The left plots in this figure correspond to spoofing detection where a spoofing signal is still present and the right plots show the same signal after elimination (Nulling) of the spoofer. The left lower plot clearly shows two peaks, while the right one corresponds to azimuth and elevation of the LOS signal, and the left one to the spoofer location (indicated in red in the corresponding sky plot).

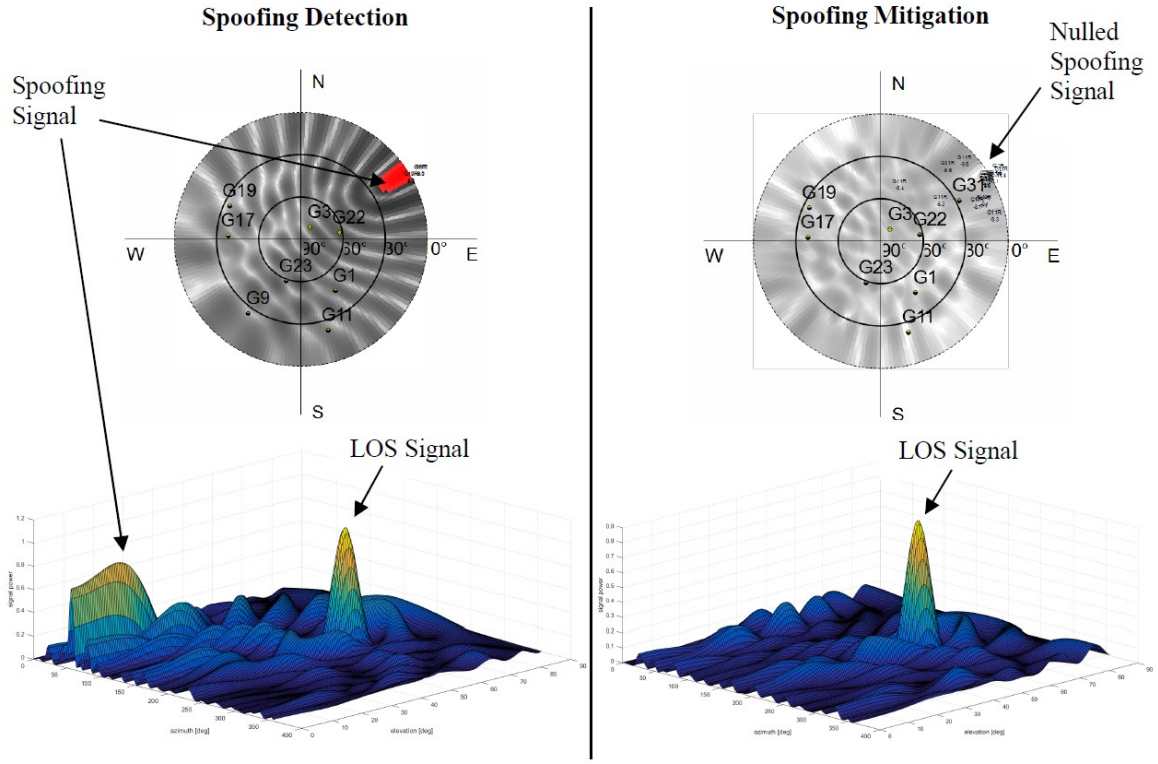

Fig. 7. Normalized signal power plotted over DoA during a spoofing attack showing the LOS signal and the spoofing signal at about an azimuth=56° and elevation=20° in the left plot and to the right the same map after nulling the spoofing signal; maps based on GPS C/A PRN 23

If the spoofing signal exhibits a certain threshold compared to the LOS signal, a spoofing signal is decided to be present. In such a case the exceeding threshold is marked red in the sky plot as shown in the upper left plot of Fig. 7 and azimuth and elevation angle is estimated to remove the spoofing signal by placing a null into this spatial direction. The spoofing elimination result is shown in the right plot of the same figure, where only the LOS component remains. All spoofing detection information is written in real-time to a file and to the status window of the SX3 software receiver, as seen in Fig. 8. The processing of different PRNs results in virtually identical spoofing signal parameters.

```
11/06/2016-22:13:24 Sequoia: Mitigated Spoofer(s) for service L1CA GPS-PRN 17 -
(1) power=2.0 dB, az=56.00°, el=18.00° - mag=1.000000; alpha=0.00°
11/06/2016-22:13:24 Sequoia: Mitigated Spoofer(s) for service L1CA GPS-PRN 19 -
(1) power=3.7 dB, az=56.00°, el=18.00° - mag=1.000000; alpha=0.00°
11/06/2016-22:13:24 Sequoia: Mitigated Spoofer(s) for service L1CA GPS-PRN 11 -
(1) power=2.5 dB, az=56.00°, el=14.00° - mag=1.000000; alpha=0.00°
11/06/2016-22:13:24 Sequoia: Mitigated Spoofer(s) for service L1CA GPS-PRN 9 -
(1) power=7.7 dB, az=56.00°, el=14.00° - mag=1.000000; alpha=0.00°
```

Fig. 8. Text log of the spoofer detection and mitigation output during processing showing the time, GNSS system/service/PRN, power referred to LOS, estimated azimuth and elevation as well as applied phase correction parameters

Position Spoofing: The goal of this scenario was to capture the victim receivers tracking loops and shift the position solution eastwards. Fig. 9 shows two position scatter plots, while the left plot refers to a classical PLL/FLL/DLL tracking loop receiver and the right one applies spoofing detection and mitigation techniques using synthetic aperture antenna processing as discussed above. The left plot clearly outlines, that it was possible to take over the control of the tracking loops and shift the position over 1.5 km away from the receiver's true position, while (a) refers to the true position when tracking the LOS without spoofing. The second circle labelled with (b) refers to the start of the spoofing attack and it shows increased position residuals indicated symbolically by a larger circle diameter. It is expected that this increased variance is caused by signal fading effects due to overlapping of the true GNSS signal and falsified direct and surface reflected spoofing signals during signal propagation. The introduced position drift was stopped after about 1.5 km offset at label (c). The implemented spoofing detection and mitigation techniques shown on the right of Fig. 9 detect the spoofing attack and prevents the victim receiver to lock on the falsified signal the receivers remains at the true PVT solution, as indicated in the right plot.

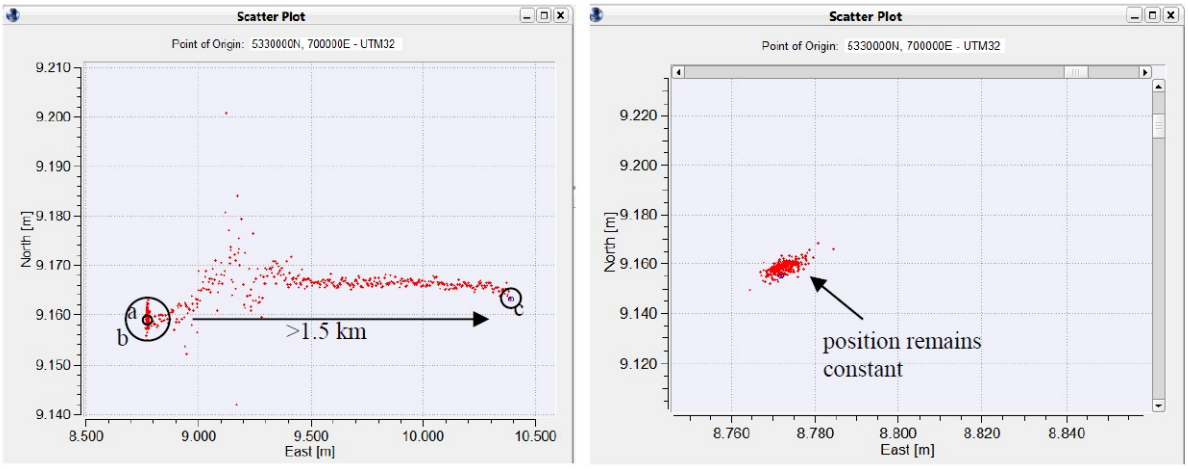

Fig. 9. Scatter plot of the position spoofing scenario driving the position eastwards with 3 m/s over 1.5 km; left plot shows the standard tracking with a static antenna and the right plot shows the rotating synthetic aperture antenna with applied spoofing mitigation techniques

SUMMARY AND OUTLOOK

By doing theoretical investigations, simulations and real-world experimentation we demonstrated within the project SETI, that a synthetic aperture antenna can reliable detect and mitigate even sophisticated spoofing attacks. The direction-of-arrival is a reliable metric to discriminate spoofing signals from line-of-sight signals. Extensive real-world spoofing experiments have been conducted and the results obtained so far seem to confirm the theoretical expectations.

Further data evaluation is planned, to verify to which extend high-end reference station data processing (e.g. PPP processing) can still be done under a spoofing attack. If this can be confirmed, the synthetic aperture processing would represent an extremely robust solution for reference stations.

REFERENCES

[1] Lin, T., Broumandan, A., Nielsen, J., O'Driscoll, C., Lachapelle, G., "Robust Beamforming for GNSS Synthetic Antenna Arrays," *Proceedings of the 22nd International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2009)*, Savannah, GA, September 2009, pp. 387-401.

[2] Pany, T., Falk, N., Riedl, B., Stöber, C., Winkel, J., Ranner, H.-P., "GNSS Synthetic Aperture Processing with Artificial Antenna Motion," *Proceedings of the 26th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2013)*, Nashville, TN, September 2013, pp. 3163-3171.

[3] R. T. Ioannides, T. Pany and G. Gibbons, "Known Vulnerabilities of Global Navigation Satellite Systems, Status, and Potential Mitigation Techniques," in *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1174-1194, June 2016.