Detection and mitigation strategies for GNSS interference attacks

Uros Bokan, Mathias Duregger, Philipp Berglez and Bernhard Hofmann-Wellenhof, Graz

Abstract

The use of global navigation satellite systems (GNSS) and the associated potential of the permanent availability of position and precise time measurements as well are playing a more and more important role in many areas of our daily life. With the steadily increasing number of applications and users, it is mandatory to think not only about the opportunities, but also about the weaknesses and risks of satellite-based positioning. Many users are currently unaware of the potential threats and their effects. In recent years, GNSS applications have become increasingly the target of deliberate interference attacks. This paper describes the impact of intentional interference (i.e., jamming and spoofing) on a software-defined receiver. In case of jamming, two state-of-the-art mitigation strategies focusing on adaptive filtering and blanking are explained in detail and their benefits are shown using simulated interference signals. In case of spoofing, different detection and mitigation techniques are discussed and two algorithms and their results are presented in detail.

Keywords: GNSS, jamming, spoofing, antenna array, notch filter, pulse blanking

Kurzfassung

Die Verwendung von globalen Satellitennavigationssystemen und das damit verbundene Potential der ständigen Verfügbarkeit einer Position sowie einer genauen Zeitmessung spielen in vielen Bereichen des täglichen Lebens eine immer größere Rolle. Durch die stetig steigende Zahl von Anwendungen und Nutzerinnen sowie Nutzern wird es zunehmend wichtiger, sich nicht nur über die Chancen, sondern auch über die Schwächen und Risiken einer satellitengestützten Positionsbestimmung Gedanken zu machen. Viele Anwenderinnen und Anwender sind sich des damit verbundenen Gefahrenpotentials und dessen Auswirkungen derzeit nicht bewusst, obwohl in den letzten Jahren GNSS-Anwendungen vermehrt das Ziel von Störattacken wurden.

In diesem Beitrag werden die Auswirkungen beabsichtigter GNSS Interferenz (d.h. Jamming und Spoofing) auf einen softwarebasierten Empfänger beschrieben. Im Fall von Jamming werden zwei unterschiedliche Mitigationsstrategien basierend auf adaptiver Filterung und Blanking im Detail erläutert sowie deren Leistungsfähigkeit anhand simulierter Interferenzsignale gezeigt. Im Fall von Spoofing werden unterschiedliche Detektions- und Mitigationsstrategien diskutiert und zwei ausgewählte Algorithmen präsentiert.

Schlüsselwörter: GNSS, Jamming, Spoofing, Antennenarray, Kerbfilter, Impulsunterdrückung

1. GNSS jamming

Jamming denotes the operation of drowning the navigation signals in high-power signals to cause loss of tracking lock and to prevent reacquisition so that a GNSS receiver cannot calculate a correct position solution. GNSS signals are particularly vulnerable to interference due to their low transmit power and the large distance between satellite and receiver. Theoretically, a 10 milliwatt jammer at a distance of 10 kilometres would be sufficient to prevent a Global Positioning System (GPS) C/A-code receiver from calculating a position solution [5]. In the civilian area, jammers, also called personal privacy devices (PPDs), are used by a wide variety of user groups to protect privacy, to shadow criminal activities or even to protect critical infrastructure. For many years, the availability and faultless operation of GNSS has been taken for granted. Jamming as well as spoofing concerned military users only. However, recent events started a gradual paradigmatic shift [6]. For example, the ground-based augmentation systems (GBAS) near airports of the United States and Taiwan were disrupted up to 117 times a day, mostly caused by truck and taxi drivers trying to hide their routes using PPDs. In 2007, a US warship entered San Diego Harbour, still activating its jammers. This resulted in failing emergency pagers, disruption and failure of the traffic management system. Jammers are cheap, easy to buy and very effective. The jamming impact of intentional interference depends on the one hand on the interference signal power and on the other hand on the spectral characteristics of the jamming signal where different types of jamming signals can be distinguished. Based on the bandwidth of the jamming signal, they can be divided into narrowband, wideband and continuous-wave interference. Based on the frequency and amplitude characteristics, a classification into continuous wave (CW), swept-continuous wave (SCW), frequency modulated (FM) and amplitude modulated (AM) jammer is possible.

According to [7] most jammers, available on the market, jam the GNSS L1/E1 band using a SCW signal. SCW signals are characterized by a constant amplitude but a periodically changing frequency using a saw tooth function. Apart from continuous jamming signals, pulsed interference signals exist. Following [8], pulsed signals are characterized by an on-off status of short duration and are mainly caused, in case of GNSS, by aeronautical radio navigation services (ARNS) like distance measuring equipment (DME) and tactical air navigation (TACAN). Pulsed signals can be described by the pulse width (length of a pulse), duty cycle (percentage of time that is occupied by the pulses) and the pulse repetition rate (number of pulses per second). More about the classification of interference can be found in [9].

1.1 Impact of GNSS jamming

Jamming signals affect both the received signal strength and the signal quality. In a first step, within the receiver internal signal processing chain, it causes a saturation of the analogue-to-digital converting (ADC) process which may result in clipping (signal amplitude exceeding the hardware capability). The automatic gain control (AGC) causes a further degradation of the useful authentic signal, reducing the signal-to-noise ratio (SNR) as well as the carrier-to-noise-density ratio (C/N0). This increases the time needed for signal acquisition (if the acquisition possible at all) and, thus, the time-to-first-fix. In addition, the number of satellites in the signal tracking is reduced and, consequently, fewer observations are available for the position calculation. The low C/N0 also causes the demodulated navigation bits to flip and therefore the decoding of the navigation message may become unsuccessful. The accuracies of the pseudorange and phase measurements are significantly reduced, due to the lower C/N0, causing a significant deterioration of the positioning accuracy up to the total failure of the positioning. In case of phase measurements, cycle slips occur more often.

1.2 Jamming detection and mitigation

A reliable detection of jamming signals is the first step towards successful mitigation. There exist different detection strategies, which are based on observing different quantities at different stages of signal processing, like AGC monitoring, monitoring of the spectral behaviour of the received signal, C/N0 monitoring, pseudoranges or Doppler monitoring or position, velocity, and time (PVT) monitoring. In order to increase the detection probability, different algorithms should be combined. After the detection, a classification is performed to obtain the spectral characteristics in order to select the most proper mitigation strategy. The methods for classification comprise short-time Fourier transform analysis as well as frequency response analysis. Once the interfering signal is detected and classified, mitigation strategies can be applied. According to literature, mitigation strategies can be defined in the frequency, in the time, and in the space-time domain, where each domain offers its advantages and disadvantages. In general, the frequency domain is used to filter out harmonic components of the interfering signal but preserving as far as possible the authentic signal. It is effective if the interfering signal occupies only a limited portion of the spectrum. The time domain is useful in case of pulsed interference. One technique, called Pulse Blanking (PB), monitors the quantized digital signal values. If a sample exceeds a defined threshold, the affected samples are set to zero. Other methods are clipping, limiting, or adaptive analogue-to-digital conversion, which are used to prevent the digital receivers from saturating, and mitigate in particular the influence of high energetic pulsed interferences. The performance of these algorithms is limited by the duty cycle. Time-space domain techniques use multiple antennas (i.e., antenna arrays) to perform a digital beamforming or null steering in order to virtually make the antenna insensitive towards the direction of interference signal arrival. Since most of the jamming signals are either SCW or pulsed, this paper focuses on the frequency and time domain, investigating the performance of Adaptive Notch Filter (ANF) and the PB algorithms.

A notch filter is a band-stop filter with a large passband frequency response and a very narrow portion of a rejection spectrum [8]. The frequency response of a notch filter is shown in Figure 1.

The notch filter is characterized by the attenuation bandwidth, which defines the bandwidth of the rejection spectrum. A low-bandwidth notch filter removes only a narrow portion of the spectrum, while the remaining signal is not or only by a few dB suppressed. If the attenuation bandwidth is set too large, the interfering signal will be attenuated and also parts of the useful signal may be suppressed. The NF represents a good strategy for mitigating interference if the jamming frequency is known and constant. In most cases, however, the frequency is an unknown parameter that changes its value over time. In this case, the ANF can be used. Adaptive notch filtering aims to estimate the unknown frequencies of periodic components buried in noise and/or retrieve such periodic components [10]. To estimate the (changing) frequencies, an adaptive unit is used. The basic structure for the bipolar ANF with an adaptive unit is shown in Figure 2.

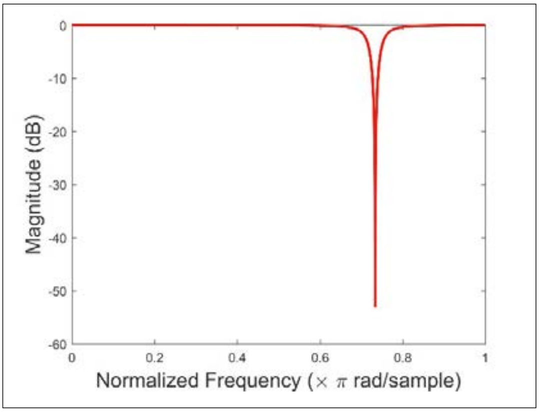

Fig. 1: Frequency response of the notch filter

In Figure 2, $y_{IF}(\mathrm{n})$ represents the input signal sample and $x_{IF}(\mathrm{n})$ denotes the filtered output signal. The numerator of the filter transfer function is defined as a moving average block and the denominator represents the autoregressive (AR) block [8]. The jammer frequency detection algorithm is based on the removal of the constraint on the location of the filter zeros in the complex plane. According to [8], their amplitude is adjusted by the adaptive unit. More information on the ANF design and implementation methods is provided in [10], [11] and [12].

Beside the attenuation bandwidth, the ANF uses an additional input parameter, called forgetting factor. The forgetting factor, which has to be chosen between zero and one, determines how fast the filter can react to frequency changes and, thus, how stable the notch frequency can be estimated over time. A forgetting factor of zero means that the ANF uses no information of the previous notch frequency estimation for the computation of the actual frequency. A forgetting factor close to one means that the ANF uses only information from the previous epoch to compute the current notch frequency. A smaller forgetting factor causes a faster reaction on frequency changes, which is very important for jammers with fast frequency changes like SCW or FM jamming signals. On the other hand, the variance of the notch frequency is increased resulting in a lower stability of the ANF

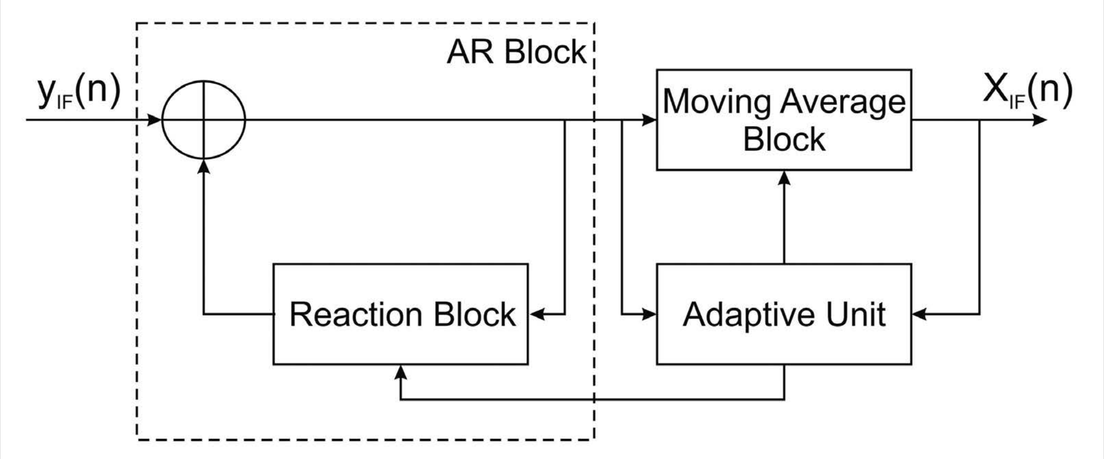

Fig. 2: Basic structure of the adaptive notch filter

and a lower quality of estimation. A larger forgetting factor will result in a more stable solution but may respond to the frequency changes with some delay. This is usually used in case of AM or CW signals.

As mentioned before, ANF is mainly used in case of continuous interfering signals. In case of pulsed interference, a time domain approach – pulse blanking (PB) – is more suitable. The PB technique is a low-cost and low-complexity pre-correlation technique that is applied on the data after the ADC and prior to the AGC and acquisition.

The quantized incoming digital signal values are constantly monitored and if a sample, containing interference, exceeds a defined threshold, the affected samples are set to zero. The pulse detection relies on the fact that the pulses are short and have a significant higher amplitude than the GNSS signal. The pulse detection may be done using different techniques, like analogue power measurements, analysing the histograms of the ADC output levels or by instantaneous power estimates [13]. From the input samples, the received power can then be calculated and compared to a decision threshold. The data can be additionally smoothed using a filter or a moving average. Furthermore, the setting of a threshold is important. The threshold has to be chosen low enough to detect (weak) pulsed interference signals, but it has to be chosen high enough to not zero too much of the useful signal. Therefore, a plausible threshold for suppression has to be found. [14] investigated the choice of a decision threshold for pulse blanking. The smallest signal degradation (-8.1 dB) happened at a decision threshold of -117.1 dBW. The PB method shown in Figure 3 demonstrates the impact on the complex signal.

The pulse blanking is not the perfect technique because during the pulse zeroing not only the pulse is suppressed, but also the useful GNSS signal. Many pulsed signals have a Gaussian

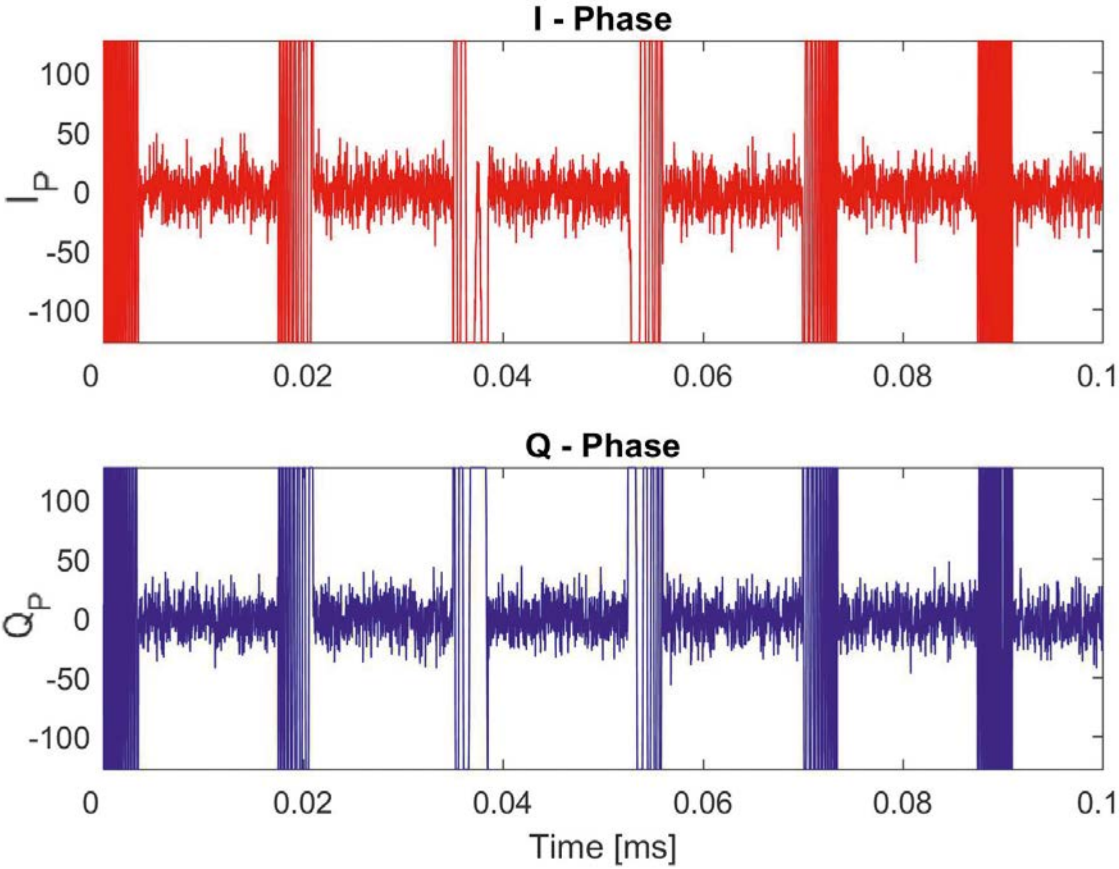

***Fig. 3:** The principle of pulse blanking (left without PB and right after PB)*

shape, which means that the pulse borders having a smaller power and amplitude are not suppressed at all [8]. Pulse blanking has to be done using a multi-bit ADC. If a single bit ADC is used, all samples have the same magnitude and it is not possible to distinguish between interference and useful signal. Furthermore, the pulse blanking should happen before the AGC. The AGC equals the signal samples and, thus, no pulse detection by amplitude discrimination is possible after that. The pulse blanking is widely-used in aviation scenarios.

2. GNSS spoofing

Spoofing denotes the manipulation, deception, or counterfeiting of GNSS signals with the aim to set a receiver to a wrong position by means of deliberately manipulated signals or to manipulate the time signal in a targeted manner. Meaconing can be considered as the simplest form of spoofing. In this case, the attacker records real GNSS signals and reradiates them again with a minor delay and with a slightly higher signal power compared to the original signal. As a result, the attacked receiver processes the delayed signals instead of the true ones and, thus, calculates an incorrect position solution. In contrast, a spoofer generates GNSS signals that match a previously set receiver position and transmits them at a slightly higher power. Depending on the effort, spoofing is classified into simple, advanced, and sophisticated attacks [8], depending on the equipment used and sophistication of the take-over algorithms.

For performing a spoofing attack, a GNSS signal simulator, sometimes in combination with a reference receiver, is used to generate and broadcast the counterfeit signals of visible satellites that are in the victim's view. In a first step, the spoofer tries to alter Doppler and code-offset of its broadcast signals to align with the ones from the real satellites. After a successful alignment, the correlation peak of the fake signal overlays with the authentic one. At this point, the power of the spoofing signals is still kept low, showing no indications to the victim. Now the attacker slowly increases the power of its signals until the victim’s receiver tracking loop locks onto them. Once the receiver has been taken over, the spoofer can drag away its correlation peak by altering the broadcast signal properties as desired, yielding a false PVT solution for the victim’s receiver.

Figure 4 shows the correlation function of one tracking channel of a victim receiver during a spoofing sequence. The blue line shows the correlation function of the authentic signal with the generated replica signal within the receiver. The three red dots indicate the early, prompt and late (EPL) correlation values. The green line represents the correlation function of the spoofing signal with the replica, while the red line shows the correlation function of the sum of the authentic and spoofing signal. At the beginning, no spoofing signal is present. At a certain point of time, the spoofing signal is visible but does not influence the EPL correlation values. Once the spoofing signal starts to interact with the authentic signal, the EPL values are affected and the power of the spoofing signal is increased. After the EPL correlations values have been taken over, a drag-off is done and the spoofer has gained control over the tracking loop. The threat of spoofing is no fiction but has rather become reality in recent years. Referring to [15] and [16], several incidents have been reported in the past.

2.1 Spoofing detection and mitigation

As in the case of jamming, detection of counterfeit signals is a prerequisite for mitigation algorithms and serves as a warning to the user not to trust the PVT solution any longer. Mitigation algorithms aim at maintaining the nominal receiver operations and trying to guarantee that no hazardously misleading information (HMI) is produced and used. In addition, some strategies aim at locating the source of the emitted false signals so that appropriate action can be taken. There exist different state-of-the-art spoofing detection methods that use different results of the internal receiver signal processing for detection. In case of static

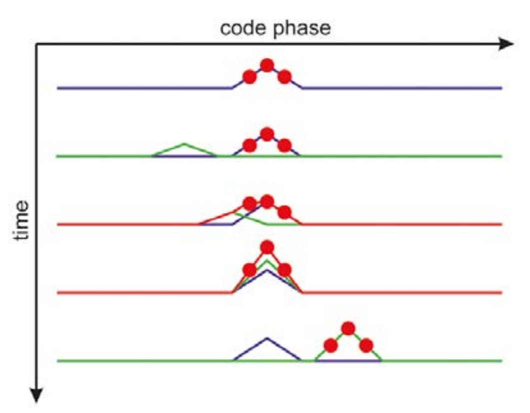

Fig. 4: Spoofing attack seen from victim’s tracking channel point of view

applications, the PVT output can be monitored. Since a spoofing signal must have higher power compared to the authentic signal to successfully spoof the receiver, the received signal power can be used as an indicator. Also, the estimated SNR and C/N0 values can be used for detection since, in case of spoofing, they are expected to be higher due to the increased signal power. In case of a dynamic application, the carrier phases of different authentic satellite signals vary differently based on the motion of the receiver and the associated direction of signal arrival. This is not the case if the spoofing signals are transmitted from a single antenna since during a spoofing attack the authentic signal is still present (cf. Figure 4). By monitoring the full cross-correlation function, instead of EPL values, multiple correlation peaks appear. Another detection and mitigation method is based on estimating the direction of the spoofing signal arrival. This can be achieved by a combined signal processing of multiple antennas, as will be described later. Other methods rely on receiver autonomous integrity monitoring (RAIM), consistency checks with other sensors (e.g., inertial measurement units) or cryptographic authentication of the satellite signal.

Within [17] a detection method based on spatial correlation of Doppler residuals was investigated. This principle exploits the property of high correlations between signals emitted by the same source. Referring to [18], measurements coming from a single source have essentially the same power spectral density and virtually the same channel gain for any space-time point. If a receiver is static, all channel gains of the authentic and spoofed signal pairs are similar and, thus, highly correlated. But as soon as the receiver starts moving, the gains based on the authentic satellites quickly de-correlate over time. This enables a distinction between authentic and spoofed signals. [17] investigated this method using Doppler measurements. By comparing the measured Doppler frequency and the theoretical one, the spatial correlation of the spoofing signals is high in case the receiver is moving. Figure 5 shows the residual Doppler values (differences between measured Doppler frequencies and theoretical ones) during a spoofing event, where only two satellites (i.e. PRN8 and PRN21) out of eight have been spoofed for a kinematic receiver.

While the residual Doppler values sourcing from the authentic satellites randomly scatter around 0 Hz, the two spoofed satellite signals show deviations of up to 80 Hz. As shown in Figure 6, the correlation values are high during the whole time span of around two minutes due to the same relative movement of the receiver. The cross-correlation coefficient between PRN8 and PRN21 is 1, while the other values are close to zero. Note that the correlation for every signal with itself (auto-correlation) also yields 1.

By using multi antenna arrays, the direction of arrival of incoming signals can be estimated. Some algorithms offer the estimation of several signal sources simultaneously depending on the number of array elements. For the case of authentic GNSS satellites, every signal is received from a different direction at the antenna. There are several types of antenna arrays. Uniform linear arrays or uniform circular arrays are the most popular ones.

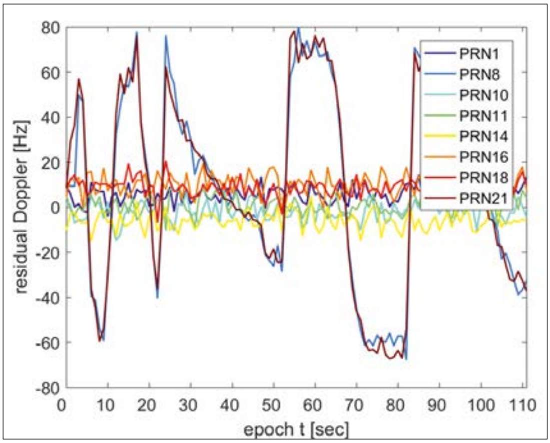

Fig. 5: Difference between measured and theoretical Doppler

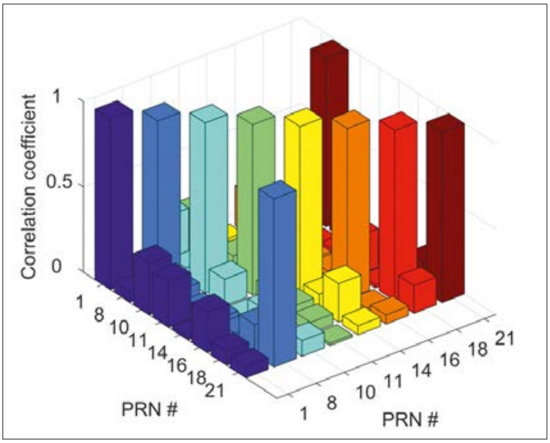

Fig. 6: Spatial correlation coefficients for residual Doppler

The more elements an array contains, the more stable is the estimation of the direction of arrival parameters. Referring to [19], the element spacing is important to avoid ambiguities in the estimated direction angles. For proper results, a spacing of equal or less than half the wavelength λ of the incoming signal is preferred. This limits the size of arrays in case of GNSS, where high frequencies for signal propagation are used. [20] describes several techniques for direction of arrival estimation. As examples, beamforming techniques and subspace-based methods are mentioned. The latter one has proven to deliver reliable results in case of closely spaced signal sources. One of these subspace-based methods is the multiple signal classification (MUSIC) algorithm. In case the algorithm detects an attack, the multi-antenna array can be utilized to determine the direction of arrival of the spoofing signals and, thus, perform a null steering. More information on the MUSIC algorithm is provided in [17].

3. Results

To evaluate the described detection and mitigation strategies, the GNSS multisystem performance simulation environment (GIPSIE®), developed by TeleConsult Austria GmbH, was used. The software is capable of simulating GNSS intermediate frequency (IF) signals. It supports all GNSS, regional and augmentation systems, which are currently available for satellite-based navigation. It enables the simulation of IF signals of multiple systems on different signal bands, the simulation of tropospheric and ionospheric path delays, and the simulation of jamming, spoofing and multipath signals. Furthermore, different RF front-ends with arbitrary settings can be simulated. It was used for this work for simulating different jamming and spoofing signals for GPS L1 C/A and Galileo E1B signals. Figure 7 illustrates a part of the graphical user interface, where the satellite systems and signals can be selected for simulation. More information on GIPSIE® can be found in [21].

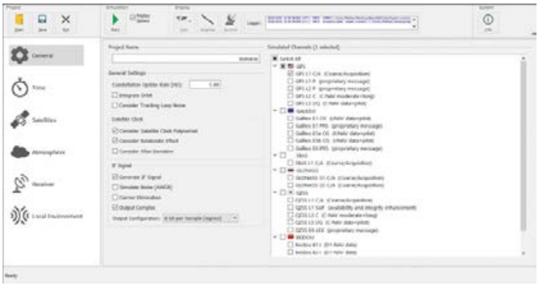

Fig. 7: *Graphical user interface of GIPSIE®*

3.1 Results of jamming mitigation

To evaluate the previously described jamming mitigation techniques, two simulations using the GIPSIE® simulator were made. In the first simulation, a swept-continuous wave jammer was simulated to evaluate the performance of an ANF. The IF signal was simulated using a sampling frequency of 40 MHz and an intermediate frequency of 0 MHz. The number of the quantization bits was set to 8. Altogether nine GPS and ten Galileo satellites were simulated. The SCW jammer has a frequency offset of 0 Hz, a sweep bandwidth of 40 MHz and a sweep duration of 18 µs. The jamming event has a duration of 10 seconds. To evaluate the effect of the jammer power on the results, the jammer power was varied. At the beginning it was set to -120 dBW. Then it is increased in the first five seconds to -110 dBW and then stays constant till the end of the interference event. The spectrogram of the simulated signal is shown in Figure 8.

The simulated signal was then processed within a software-defined GNSS receiver [22]. The C/N0 during the interference event for Galileo is presented in Figure 9.

During the interference event the C/N0 decreases depending on the jamming signal power: the stronger the jamming power, the lower the C/N0. The receiver loses track of some satellites, due to the jamming signal characteristics and the high power. Figure 10 shows the differences of the

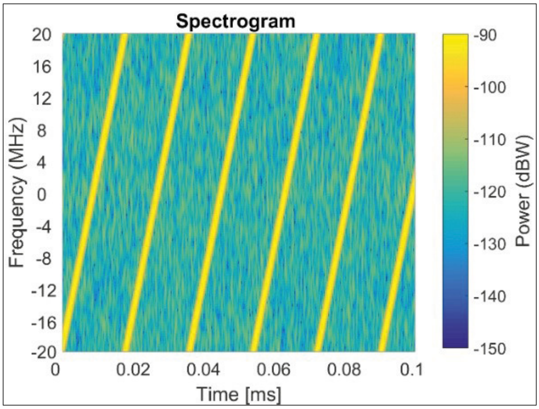

Fig. 8: *Spectrogram of the simulated SCW jammer*

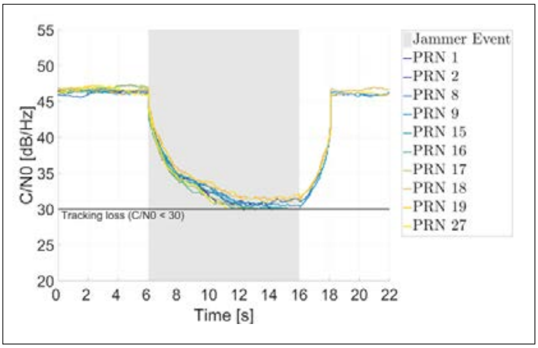

Fig. 9: C/N0 of the Galileo satellites without activating the ANF

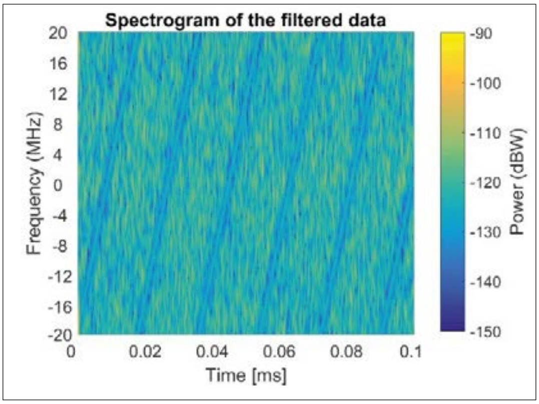

Fig. 11: Spectrogram of the filtered data

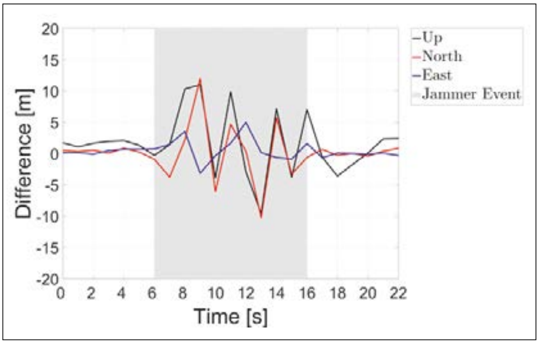

Fig. 10: Difference to the reference position during the SCW jamming event

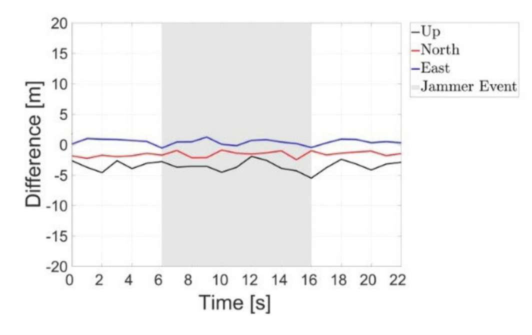

Fig. 12: Coordinate differences to the reference position after filtering out the jamming signals

computed positions with respect to the simulated reference position during the jamming event.

The coordinate differences to the reference position get higher during the interference event. Due to the low C/N0, the tracking gets inaccurate resulting in erroneous pseudorange measurements for all satellites. Furthermore, the tracking to some satellites is lost, which means that less observations for the least-squares-adjustment are available, worsening the geometry. In the next step, the ANF was applied on the simulated signal. Different combinations of the input parameters were tested. The optimum solution – chosen for further calculations – was achieved using a forgetting factor of 0.3 and an attenuation bandwidth of π/3. The spectrogram of the filtered signal is shown in Figure 11.

Figure 12 shows the coordinate differences of the obtained position solution with respect to the reference after applying the ANF.

The ANF filters out the interference part of the incoming signal which increases the C/N0 values. This prevents the receiver from losing tracking to satellites; therefore a stable PVT solution can be obtained. However, the C/N0 is slightly lower compared to the interference-free event. The reason for that is that the ANF suppresses not only the interfering signal, but it suppresses also a part of the useful signal. This reduces the carrier power and decreases the C/N0.

For evaluating the PB algorithm, a pulsed jamming signal was simulated using the GIPSIE® simulator, with a pulse width of 3.5 μs and a duty cycle of 0.6. The effect of PB on the simulated signal was already shown in Figure 3. First, the data were processed using the software-defined receiver without applying the pulse blanking algorithm. The C/N0 during this interference event is shown in Figure 13.

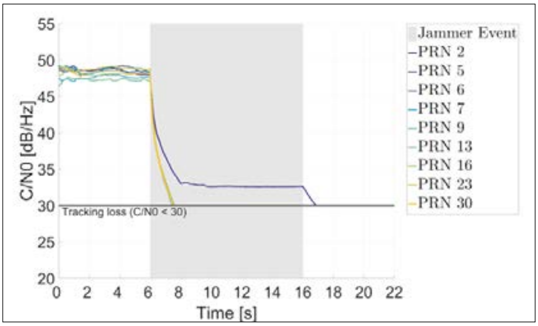

Fig. 13: *C/N0 of the pulsed interferer without pulse blanking*

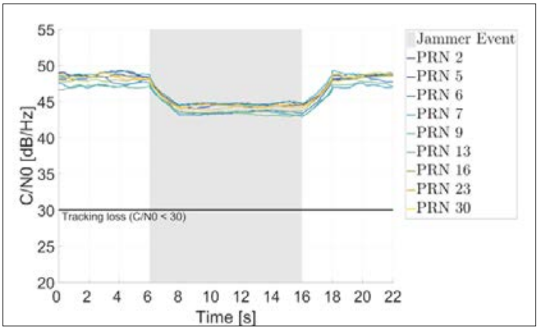

Fig. 14: *C/N0 after pulse blanking*

Due to the high duty cycle, the receiver loses track of all satellites. After applying the BP algorithm on the simulated signal, every satellite could be kept in tracking and only a small reduction of the C/N0 is visible, as shown in Figure 14.

It has to be mentioned that the duty cycle is an important parameter for the signal processing. The higher the duty cycle, the smaller is the amount of useful received signal, which causes worse tracking and positioning quality. The main problem of the pulse blanking algorithm is the pulse detection, especially the choice of the decision threshold.

3.2 Results of spoofing detection

Based on the investigation of residual Doppler correlations, an effective detection and mitigation algorithm has been developed and presented in [17]. For investigating the performance of the proposed algorithm, a scenario has been simulated within the software GIPSIE®. For this scenario, eight authentic GPS C/A-code satellite signals on the L1 frequency have been simulated together with the same set consisting of spoofed signals. Furthermore, a receiver movement with an arbitrary motion pattern was simulated. These two sets imitated all signals tracked inside a software-defined radio during an attack. Based on the proposed algorithm in [17], a coarse classification of the individual signals is performed by using the measured C/N0 values. In case a false classification was made, a further distinction through iteration was executed. For this test, a worst case scenario has been generated, where two sets (eight satellites per set) were misclassified by the algorithm. This resulted in sets consisting of four authentic and four spoofed signals each.

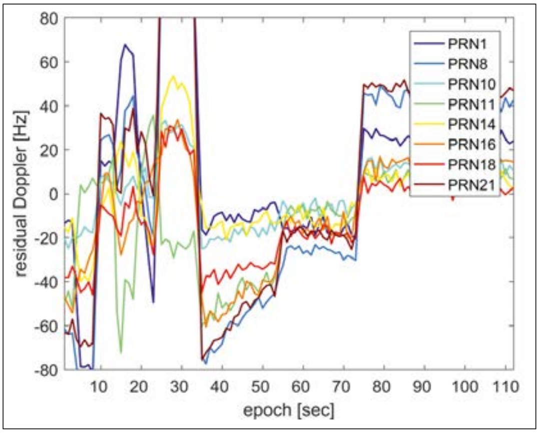

Fig. 15: *Doppler residuals for misclassified PVT set (50% authentic, 50% spoofed)*

Figure 15 shows the resulting Doppler residuals for a time span of about two minutes, where the theoretical Doppler values were processed using a spoofed PVT output due to misclassification. PRN1 to PRN11 are authentic satellites, whereas PRN14 to PRN21 are spoofed. Afterwards, the algorithm started its sorting process. The whole time series was divided into data snapshots of equal length, where each snapshot was processed individually. Figure 16 shows Doppler residuals of the two processed data sets, where the first half of the time series has already been sorted correctly.

As can be seen on the left, no correlations between the single signal pairs are present. After 55 seconds, the Doppler residuals on the right exceed the values of 80 Hz due to the inconsistency of the data sets. Figure 17 shows the final result after the algorithm has processed all data snapshots. As expected, the algorithm has correctly classified the signals. The Doppler residuals show a highly correlated pattern for the spoofed set, representing the relative motion of the receiver

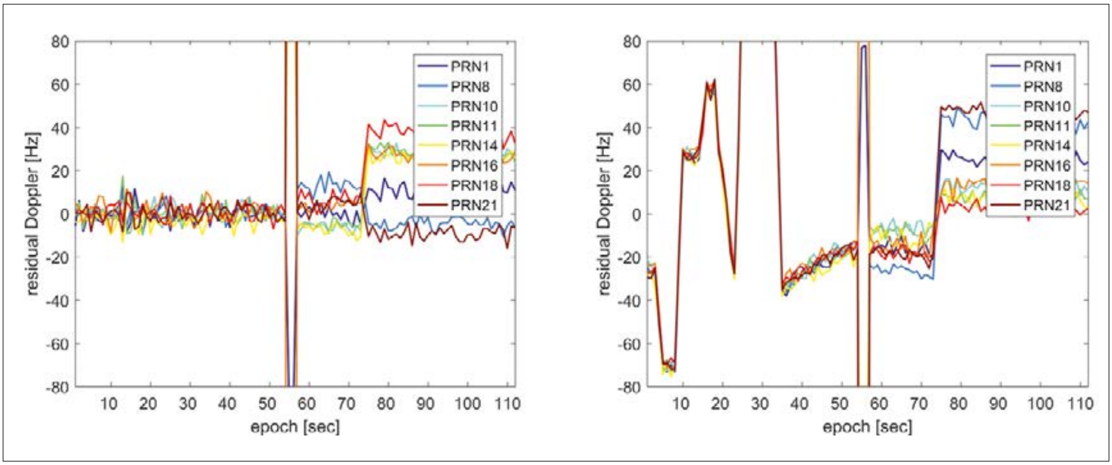

***Fig. 16:** Rearranging misclassified authentic (left) and spoofed (right) PVT set*

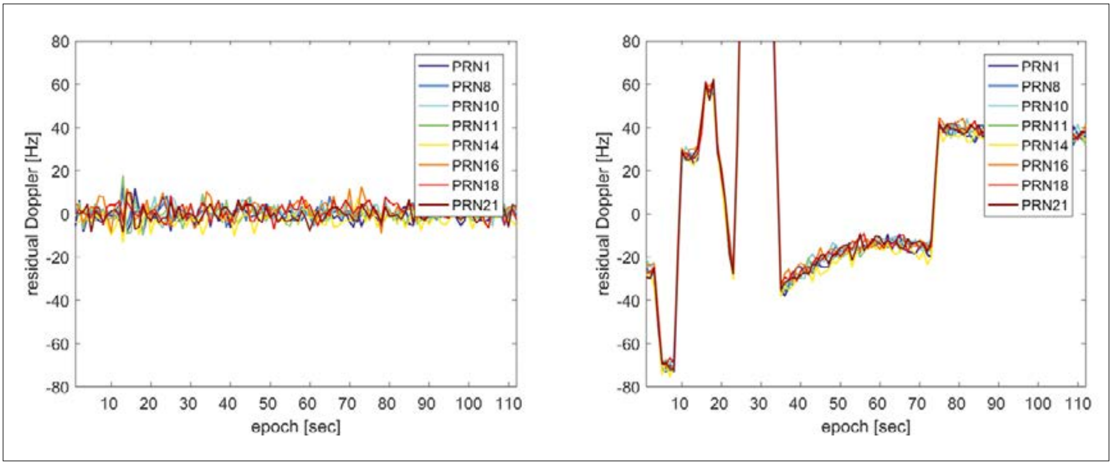

***Fig. 17:** Correctly sorted authentic (left) and spoofed (right) PVT set*

with respect to the spoofer. The sudden jumps in the values occur when the receiver changed its direction in the trajectory.

For assessing the performance and accuracy of the previously discussed MUSIC algorithm, three spatial distributed spoofing signals were simulated using GIPSIE®. The uniform circular array was simulated as eight individual receivers within a radius of 9 centimetres.

The reference azimuth and elevation between the centre of the uniform circular array and the respective spoofer are listed in Table 1. Furthermore, the relative power between the emitted counterfeit signals and the authentic ones is given along with the distances. As can be seen, the distances between every spoofer and the centre of the uniform circular array is the same.

A MUSIC estimation has been performed where signals from the three spoofing signals where

	Azimuth [°]	Elevation [°]	Rel. power [°]	Distance [m]
Spoofer 1	136	36	20	1000
SP2	45	85	16	1000
SP3	295	12	18	1000

***Tab. 1:** direction of arrival properties of simulated spoofing signals*

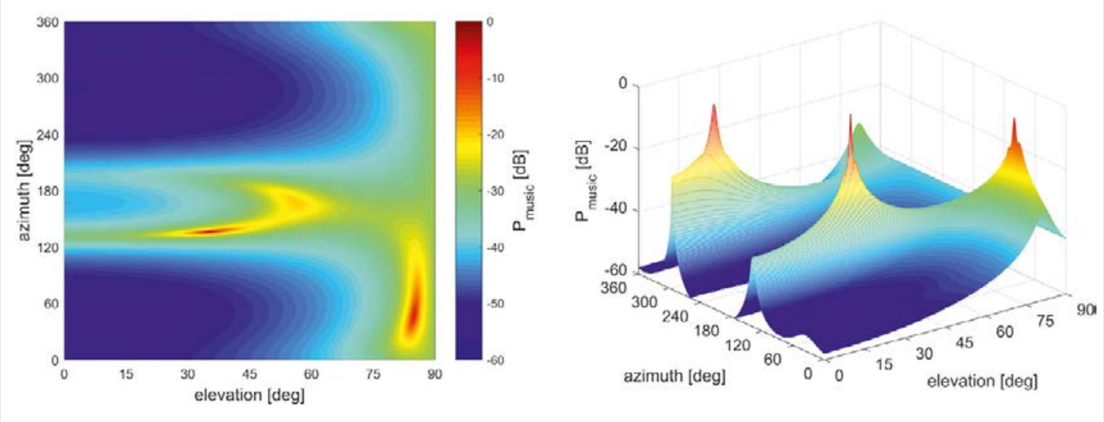

Fig. 18: *2D (left) and 3D (right) MUSIC spectrum for three spoofing signals*

arriving at the array. For peak searching, a grid resolution of 0.5 degrees was used. Beamforming was applied, to increase the performance of the algorithm as well as the spatial resolution of the spectrum in case of coherent signals. Figure 18 shows the respective 2D and 3D MUSIC spectrum in the presence of the three spoofing signals.

On the 3D spectrum, the x- and y-axis denote the azimuth and elevation angle respectively, while the z-axis shows the spectrum power in decibel. The algorithm had no problem determining the correct angle pairs of the sources when compared to Table 1, where peaks close to the reference values for azimuth and elevation are visible. It is remarkable that the second spoofer has the worst resolution, especially in its azimuth. The reason for this is the weaker power of this spoofer compared to the others (4 dB weaker as compared to Spoofer 1 and 2 dB weaker as Spoofer 3). All present spoofing signals are correlated with a connecting region where the spectrum is around -30 dB.

4. Conclusions

The impact of jamming and spoofing is described. In order to provide a reliable and robust PVT solution, GNSS interference caused by jamming and spoofing has to be detected, classified and then mitigated.

Referring to jamming, the adaptive notch filter (ANF) and pulse blanking (PB) successfully suppress the jamming signals. This results in a reduction of the noise level of the signal and causes an increase of the C/N0 and a more accurate PVT solution. In addition, in many cases it prevents the receiver from losing the tracking to the satellites and enables a calculation of the PVT solution.

The ANF estimates the interfering frequency and filters it out. The choice of the input parameters of the ANF, the forgetting factor and the attenuation bandwidth, is very important.

The PB algorithm shows good results for mitigating pulsed interference. The main problem of PB is the pulse detection, which might reduce the performance of the algorithm.

Referring to spoofing, the correlations of Doppler residuals have been exploited to successfully detect an ongoing spoofing attack and further mitigate it by correctly classifying the tracked signals into authentic and spoofed sets. A direction of arrival estimation based on multiple signal classification (MUSIC) for several spoofing signals has been successfully demonstrated with a simulated antenna array. With the simulated eight-element array, directions of arrival for three spoofing signals were simultaneously determined without performance losses in terms of accuracy and computation time.

Acknowledgments

The research work described here was carried out within the scope of the projects "Detection, countermeasures and demonstration of GNSS spoofing" (DECODE) [23] and "Impacts and countermeasures of Austrian PRS application scenarios in GNSS denied environments (PRSAustria)" [24]. The projects DECODE and PRSAustria were successfully completed in 2018 and received funding from the Federal Ministry of Transport, Innovation and Technology (BMVIT) under the responsibility of the Austrian Research Promotion Agency (FFG) within the framework of the Austrian Space Application Program (ASAP). The authors would like to thank BMVIT for the financial support, FFG for the profes-

sional handling as well as all involved project partners for the excellent cooperation.

References

[1] *Jones M (2011)*: The Civilian Battlefield – Protecting GNSS Receivers from Interference and Jamming. Inside GNSS, March/April.

[2] *Berglez P, Katzler-Fuchs S (2015)*: The PRS – Secure EU Satellite Navigation for Government Use. Eingeladener Vortrag bei der Informationsveranstaltung des Bundeskanzleramts, BMVIT, Vienna, 12. October.

[3] *Mitch R, Dougherty R, Psiaki M, Powell S, O'Hanlon B (2011)*: Signal Characteristics of Civil GPS Jammers. In: Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2011), Portland, Oregon, September 20-23: 1907-1919.

[4] *Dovis F (2015)*: GNSS Interference Threats and Countermeasures. Artech House, Boston London.

[5] *Bartl SM (2014)*: GNSS Interference Monitoring - Detection and classification of GNSS jammers. Master thesis, Institute of Navigation, Graz University of Technology, Austria.

[6] *Regalia PA (2010)*: A Complex Adaptive Notch Filter. In: IEEE Signal Processing Letters 17(11): 937-940.

[7] *Regalia PA (1991)*: An Improved Lattice-based Adaptive IIR Notch Filter. In: IEEE transactions on signal processing 39 (9): 2124-2128.

[8] *Bokan U (2018)*: Mitigation Strategies for GNSS Jamming Attacks. Master thesis. Institute of Geodesy, Graz University of Technology, Austria.

[9] *Hegarty C, Dierendonck AJ van, Bobyn D, Tran M, Kim T, Grabowski J (2000)*: Suppression of Pulsed Interference Through Blanking. In: Proceedings of the IAIN World Congress and the 56th Annual Meeting of The Institute of Navigation (2000), San Diego, California, June 26 - 28: 399 - 408.

[10] *Raimondi M, Julien O, Macabiau C, Bastide F (2006)*: Mitigating Pulsed Interference Using Frequency Domain Adaptive Filtering. In: Proceedings of the 19th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2006), Fort Worth, Texas, September 26 - 29: 2251 - 2260.

[11] *Shepard D, Bhatti JA, Humphreys TE (2012)*: Drone Hack: Spoofing Attack Demonstration on a Civilian Unmanned Aerial Vehicle. In: GPS World. Aug 1. Available at www.gpsworld.com/drone-hack.

[12] *Psiaki ML, Humphreys TE (2016b)*: GPS Lies. Available at https://spectrum.ieee.org/telecom/ security/protecting-gps-from-spoofers-is-critical-to-the-future-of-navigation.

[13] *Duregger M (2018)*: Detection Strategies for GNSS Spoofing Attacks. Master thesis. Institute of Geodesy, Graz University of Technology, Austria.

[14] *Broumandan A, Jafarnia-Jahromi A, Dehghanian V, Nielsen J, Lachapelle G (2012)*: GNSS Spoofing Detection in Handheld Receivers based on Signal Spatial Correlation. In: Proceedings of the 2012 IEEE/ION Position, Location and Navigation Symposium. Myrtle Beach, South Carolina. Apr 24-26.

[15] *Broumandan A, Lin T, Moghaddam A, Lu D, Nielsen J, Lachapelle G (2007)*: Direction of Arrival Estimation of GNSS Signals Based on Synthetic Antenna Array. In: Proceedings of the 20th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2007). Fort Worth, Texas. Sept 25-28.

[16] *Krim H, Viberg M (1996)*: Two Decades of Array Signal Processing Research. In: IEEE Signal Processing Magazine 13.4: 67-94.

[17] *TeleConsult Austria (2019)*: GIPSIE - GNSS Multisystem Performance Simulation Environment. Available at https://www.tca.at/en/products/gnss-processing/gipsie.

[18] *Berglez P (2013)*: Development of a Multi-frequency Software-based GNSS Receiver. PhD thesis. Institute of Navigation, Graz University of Technology, Austria.

[19] *TeleConsult Austria GmbH (2016)*: Detection, Countermeasures and Demonstration of GNSS Spoofing (DECODE). Available at www.tca.at/decode-4-de.

[20] *TeleConsult Austria GmbH (2016)*: Impacts and Countermeasures of Austrian PRS Application Scenarios in GNSS Denied environments (PRSAustria). Available at http://www.tca.at/prsaustria-4-de.

Contacts

Dipl.-Ing. Uros Bokan, TeleConsult Austria GmbH, Rettenbacher Straße 22, A-8044 Graz, Austria.

E-Mail: uros.bokan@tca.at

Dipl.-Ing. Mathias Duregger, TeleConsult Austria GmbH, Rettenbacher Straße 22, A-8044 Graz, Austria.

E-Mail: mathias.duregger@tca.at

Dipl.-Ing. Dr. Philipp Berglez, TeleConsult Austria GmbH, Rettenbacher Straße 22, A-8044 Graz, Austria.

E-Mail: philipp.berglez@tca.at

Univ.-Prof. Dipl.-Ing. Dr. Dr.h.c.mult. Bernhard Hofmann-Wellenhof, Graz University of Technology, Steyrergasse 30, A-8010 Graz, Austria.

E-Mail: hofmann-wellenhof@tugraz.at

vgi