Time Synchronized Signal Generator GNSS Spoofing Attacks against COTS Receivers in over the Air Tests

Ronny Blum[1], Nikolas Dütsch[1], Jürgen Dampf[1], Thomas Pany[1]

[1] Institute of Space Technology and Space Applications, Universität der Bundeswehr München, Germany

BIOGRAPHIES

Ronny Blum received his master in Physics from the University of Basel, Switzerland. Since then he worked at Würth Elektronik in the field of signal transmission and later on at the Forest Research Institute in Freiburg im Breisgau in the field of GNSS reception within the forest. 2017 he joined the Universität der Bundeswehr München, where he is working in the field of GNSS software receiver with research topics in the field of spoofing, Signal Quality Monitoring and Galileo PRS.

Nikolas Dütsch received his master in Electronics from the Friedrich-Alexander-University in Erlangen/Nuremberg, Germany. Since then he started working as a systems engineer in the field of Galileo PRS at IABG mbH. Since 2020 he is working as research associate at the Universität der Bundeswehr München with research topics in the field of anti-jamming and anti-spoofing techniques for GNSS receivers.

Jürgen Dampf works as a software development engineer at Rohde und Schwarz GmbH & Co. KG in the department for high-end spectrum analysis. In parallel he works as a research associate at the Universität der Bundeswehr München. Formerly he worked as a GNSS R&D engineer at Trimble Terrasat GmbH, as CTO at IGASPIN GmbH and as GNSS system engineer at IFEN GmbH. His research topics range from GNSS reflectometry, sensor fusion, integrated navigation, beamforming, efficient GNSS signal processing algorithms and jamming/spoofing signal generation and mitigation techniques. In his PhD at the Graz University of Technology he is investigating the topic of Bayesian Direct Position Estimation (BDPE) for GNSS receivers.

Prof. Thomas Pany is with the Universität der Bundeswehr München at Space Systems Research Center (FZ-Space) where he leads the satellite navigation unit LRT 9.2 of the Institute of Space Technology and Space Applications (ISTA). He teaches navigation focusing on GNSS, sensors fusion and aerospace applications. Within LRT 9.2 a good dozen of full-time researchers investigate GNSS system and signal design, GNSS transceivers and high-integrity multi-sensor navigation (inertial, LiDAR) and is also developing a modular UAV-based GNSS test bed. ISTA also develops the MuSNAT GNSS software receiver and recently focuses on Smartphone positioning and GNSS/5G integration. He has a PhD from the Graz University of Technology and worked in the GNSS industry for seven years. He authored around 200 publications including one monography and received five best presentation awards from the US institute of navigation. Thomas Pany also organizes the Munich Satellite Navigation Summit.

ABSTRACT

In this work we present the results of over the air spoofing experiments with common Commercial of the Shelf (COTS) receivers. In the literature only very few over the air transmissions of spoofing signals were treated, most likely because of the missing sending permission. Therefore this paper analyses some successful spoofing experiments with over the air transmission. Signal generator spoofing is the generation and emission of artificial authentic Global Navigation Satellite System (GNSS)-signals with a signal generator, which tries to imitate the real satellite signals as good as possible to induce a wrong time and/or position output on the victim receiver. The artificial signals must have a higher amplitude at the target position than the authentic signals to be tracked from the receiver. We investigated synchronized attacks with a purchasable Jamming and Spoofing generator from [14], which is able to perform a synchronized spoofing attack to real satellite signals and by now Galileo E1B/C and GPS L1 C/A signals can be spoofed. The spoofing device estimates the navigation bits and code phase in real time. The position could be shifted kilometres away from the initial position. The behaviour of several anti-spoofing parameters under the spoofing attack were analyzed, amongst others some tracking parameters like the Code Minus Carrier (CMC), Code rate of the replica (CRR), Doppler, discriminator values, In-Phase (I) and Quadrature (Q) channel power and C/N_0. Additionally several Signal Quality Monitoring (SQM) parameters were tested, the Single Sided Ratio metric (SRM), Ratio Metric (RM), Delta Metric (DM), Double Delta Metric (DDM), Moving Variance of Delta Metric (MV) and the

Threshold Fluctuation Metric (TFM), presented in [9]. For this specific spoofing experiment all considered anti-spoofing parameters and metrics showed a significant deviation when the spoofing started, which allows for threshold-based detection methods. One receiver could be spoofed with Galileo E1B/C and GPS L1 C/A signals, even if it tracked in parallel authentic Beidou and GLONASS satellites on the L1 band. This illustrates that a spoofer not necessarily need to spoof all GNSS's which are supported by the receiver, in order to perform a successful spoofing attack. The position shift of the receivers was in the kilometer range.

Keywords: GNSS, spoofing, over the air, spoofing defense, anti-spoofing, signal generator attack

I. INTRODUCTION

Like also for jamming and interference, GNSS signals are vulnerable to spoofing due to the low signal power. Spoofing is the intended manipulation of the navigation solution of a GNSS receiver, which is the estimated Position, Velocity and Time (PVT). Spoofing is a potential safety threat to several applications in many sectors like transportation, communication, law enforcement, military, financial and energy. Table 1 gives an overview of applications which are potential vulnerable to spoofing. Hereby, p/t indicates if the application relies on the position or time solution of the GNSS receiver. Since GNSS can provide the absolute time on the nanosecond level, many safety critical time applications became dependent on a correct navigation solution of the receiver.

For example, GNSS based monitoring of fishing could be manipulated by spoofing. Fishing is normally only be allowed in a certain area, but the position could be spoofed such that the vessel stays in this allowed area while fishing in forbidden areas. Since 2005 fishing waters are controlled by the European Union (EU) and operators of fishing vessels with more than 15 meters in length require to carry a GNSS-based monitoring system. This system records the route of the vessel and automatically provides the data to the fisheries monitoring center of the EU member state. The registration of the ship includes knowledge about the registration state which allows to identify in whose waters the vessel is allowed to fish [1]. Furthermore, military enemy ships could be spoofed away from certain targets or port container logistics could also be affected by spoofing. Some port cranes work with GNSS, which could be spoofed to disrupt the automatic container logistics. Cargo ships could be hijacked by disguising the true location of the container or ship.

The automatic GNSS based surveillance broadcast of air transport could be manipulated by spoofing or aircraft can be affected in the most critical flight phases during approach and departure. Furthermore, the surveillance of trucks is a vulnerable area, as truck drivers could manipulate the monitored tracked route in order to avoid the mandatory rest periods or illegally dump trash.

The upcoming autonomous driving could also be affected by spoofing. Autonomous driving cars rely on multi-sensor fusion, whereas one sensor is the GNSS receiver contributing with an absolute and accurate PVT. If the PVT of the GNSS receiver diverges from all other sensors may indicate a present spoofing attack. The presence of a spoofing attack could lead to cumulative sensor errors, which applies also for jamming and which can potentially lead to accidents.

A taxi driver could manipulate his own monitored position of the car to pretend being at a popular place in the city in order to get more customers. In this way he could steal costumers from other taxi drivers. The same principle could be used in car sharing, when offering the own car or a fleet of cars to others. Cars could be offered at popular places while being at that moment at a different location, and which is driven to offered place in case of a customer request.

Also, the law enforcement is a vulnerable area to spoofing. The GNSS position or time information as evidence material or the law enforcement equipment with time-based software licenses could be manipulated.

The stock exchange requires a precise time. Wrong arbitrages could be generated by manipulating the time in synchronization systems.

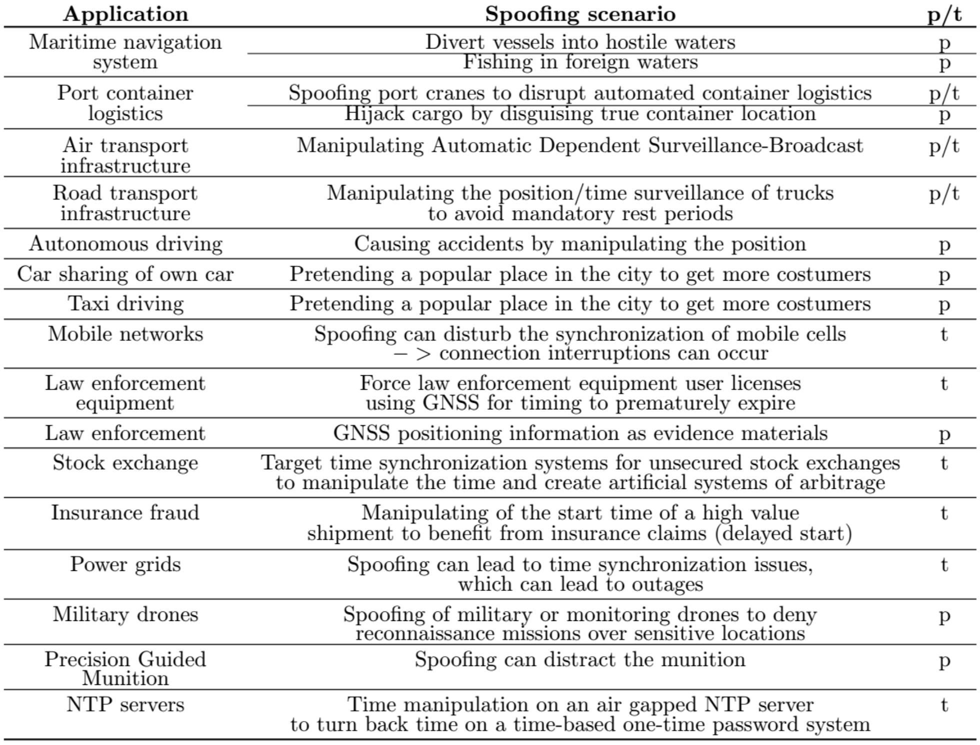
An insurance fraud of a high value shipment could be to manipulate the start time of the shipment. A delay in the start time leads to an insured event, which can be huge amounts of money depending on the shipment.

The main danger might be in military applications. Drone spoofing, which also occurred in the past, is one case. Enemy drones could be forced to land in the own territory or could be forced to turn away from the own territory. One could deny reconnaissance missions over special sensitive locations, that should be kept secret. Also, GNSS based precision guided munition could be spoofed and distracted from certain areas. This protection behavior is exercised in Russia and Syria, in this case only by denial of service [2].

A time-based password system is a further application that is potentially vulnerable to spoofing. If the time of a Network Time Protocol (NTP) server is turned back, the password could be reused or be stolen.

Power grids are another safety critical application, which might be spoofed. The grids are supported from GNSS time to synchronize each other by using Phasor Measurement Units (PMU). A PMU is used to estimate the magnitude and phase angle of the voltage and current in the electricity grid using a common time source for synchronization. If the time is manipulated, wrong information is delivered to the power grid. This can lead to wrong actions and decisions at the power grid surveillance, which can result in outages. Papers which investigate the spoofing threat to power grids and possible detections can be found in [3], [4], [5] and [6].

Table 1: Overview of critical applications that are vulnerable to spoofing



Application	Spoofing scenario	p/t
Maritime navigation system	Divert vessels into hostile waters	p
	Fishing in foreign waters	p
Port container logistics	Spoofing port cranes to disrupt automated container logistics	p/t
	Hijack cargo by disguising true container location	p
Air transport infrastructure	Manipulating Automatic Dependent Surveillance-Broadcast	p/t
Road transport infrastructure	Manipulating the position/time surveillance of trucks to avoid mandatory rest periods	p/t
Autonomous driving	Causing accidents by manipulating the position	p
Car sharing of own car	Pretending a popular place in the city to get more costumers	p
Taxi driving	Pretending a popular place in the city to get more costumers	p
Mobile networks	Spoofing can disturb the synchronization of mobile cells $->$ connection interruptions can occur	t
Law enforcement equipment	Force law enforcement equipment user licenses using GNSS for timing to prematurely expire	t
Law enforcement	GNSS positioning information as evidence materials	p
Stock exchange	Target time synchronization systems for unsecured stock exchanges to manipulate the time and create artificial systems of arbitrage	t
Insurance fraud	Manipulating of the start time of a high value shipment to benefit from insurance claims (delayed start)	t
Power grids	Spoofing can lead to time synchronization issues, which can lead to outages	t
Military drones	Spoofing of military or monitoring drones to deny reconnaissance missions over sensitive locations	p
Precision Guided Munition	Spoofing can distract the munition	p
NTP servers	Time manipulation on an air gapped NTP server to turn back time on a time-based one-time password system	t

There exist several different types of spoofing from low sophisticated (for example Record and Replay Attack and meaconing, treated in [7]) to highly sophisticated (synchronized signal generator attacks with multiple antennas). In this paper an intermediate to highly sophisticated attack is investigated, the time-synchronized signal generator attack with a single transmission antenna.

The code phase and navigation bits from the authentic signal are estimated from the spoofing device. In order to align the spoofing signal with the authentic signal, the (1) GNSS time, the (2) distance from the spoofer to the victim receiver and the (3) navigation data bits need to be known precisely. Therefore, the spoofing device uses an integrated GNSS receiver which delivers the PVT and navigation data bits in order to allow a precise alignment of the clock, to determine and compensate for the transmission delay and to predict the navigation data bits based on previous known sequences. The setup of the spoofer consists of a software receiver with an integrated spoofing feature running on a conventional Personal Computer (PC) or notebook, two Software Defined Radios (SDR), a synchronization Radio Frequency (RF) frontend and a transmission RF frontend, both are connected to a GNSS antenna, one reception and one transmission antenna. Figure 1 illustrates the attack with an USRP from Ettus Research as transmission frontend. The navigation bits are extracted from the GNSS source of the synchronization frontend or can also be downloaded from the internet. If the phase center of the victim antenna is known precisely, the spoofer could also generate a carrier phase synchronized attack, but the complexity of this approach is very much higher. In this setup, the baseband spoofing signal is generated with the PC, converted to an analogue signal and mixed up to the carrier frequency using the USRP transmission frontend. There are also other concepts of a spoofing device possible or imaginable. In general, when the location of the target is known, a good code phase estimation can be achieved. In such a case the correlation function of the spoofer is well aligned with the authentic one. The alignment avoids position and time jumps, which could be detected. For a successful spoofing attack, the alignment has to be better than 1 chip (1µs), and deviations of more than around 10 ns could be detected based on our empirical evaluation of the spoofing trials. As mentioned above, the better the alignment, the better the chance of not being detected. In our best knowledge there exist at the moment no COTS receivers which have implemented detection algorithms that can detect time deviations smaller than 1µs. The knowledge to build a high-end spoofing system is considered to be very high and a device, even if it is purchasable today, is very costly

(>20000 US Dollars). However, renting such a device for a certain time can be cheaper. Since the spoofer uses one antenna, all the fake satellite signals are coming from the same spot, which is a potential weakness of this attack. A multi-antenna system or a synthetic aperture could detect the attack and mitigate the spoofing signal by filtering the direction of the spoofing signals, although these systems are very expensive. A perfect code and carrier phase-synchronized signal generator attack do not show the common fading effects in a static spoofing phase due to the constant overlap of spoofing and authentic signal. However, this is not the case if a moderate or low power spoofer shifts the position away, because then the relative phase of authentic and spoofing signal is changing. For the signal generator attacks, successful spoofing typically only works, if all satellite systems are used, which are also used by the target receiver. Otherwise there occur inconsistencies between the code phases of the satellites from different systems, which in general leads to an unsuccessful attack. But there are exceptions, which we found in this paper work.

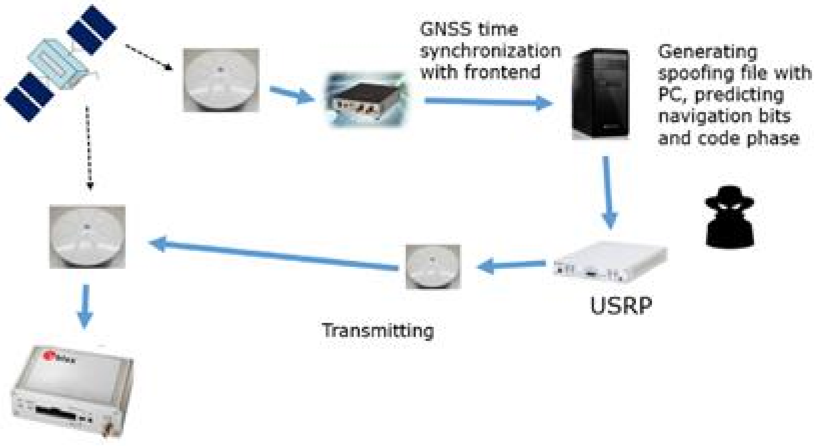

GNSS time synchronization with frontend
Generating spoofing file with PC, predicting navigation bits and code phase
USRP
Transmitting

Figure 1: Schematic structure of the signal generator attack with one transmission antenna

Since in the open literature either spoofing attacks over a cable setup or with a repeater in an indoor environment or the famous Texas Spoofing Test Battery (TEXBAT [19]) spoofing data from the Radionavigation Laboratory at the University of Texas at Austin (6 different spoofing attacks [8], [16], [17]) are treated, this paper analyzes a self-made over the air time synchronized spoofing attack. An example for a paper in which the TEXBAT was used can be found in [8].

II. THEORY, METHODS AND MEASUREMENTS

II.1 Signal model and window of overlap

A spoofing attack can be explained in the correlation process in the receiver. When the spoofer signal has at least a slightly higher signal amplitude than the authentic signal, the receiver switches to the correlation peak of the spoofer. During the transition period and as long as the spoofing and authentic correlation function overlap, the resulting correlation function in the receiver gets distorted and fluctuations occur, as shown in Figure 2. This means, even when the spoofing signal is tracked by the receiver, fluctuations occur due to a different Doppler and code phase offset, which is required to modify the PVT of the receiver. Fluctuations and deformations of the resulting correlation functions will occur, as long as the correlation functions are not clearly separated from each other in the correlation domain. This is also the case for a high sophisticated spoofer with a perfect alignment of the code phase, Doppler and signal power. Therefore, we think that fluctuations occur in most cases, even for the highest sophistication of spoofing, because the position and/or time has to be shifted away for a successful attack. If the gain of the spoofer is very high, these fluctuation effects are reduced or cannot be seen at all, because the spoofing signals becomes dominant. It should be noted that such an attack can be easily detected by observing the receiver Automatic Gain Control (AGC), which will change significantly in order to adapt to the strong spoofing signal. But the range of the AGC is limited and once it is exceeded, signal tracking interruptions can be observed, which is also noticeable for a static open sky antenna. In [3] we have shown, that the fluctuation metric is capable of detecting any shifting attempt of the spoofer. During the shifting process, the correlation functions from the authentic and spoofing signal move apart until they are completely separated from each other. After this point, none of the investigated metrics can detect the attack, because the fluctuations only occur during the overlap. It should be noted, that imperfect or unsynchronized spoofing attacks (no overlap of the correlation functions) can be detected by monitoring Doppler-delay maps, which can be produced efficiently with Fast Fourier Transform (FFT) acquisition techniques or with a Synthetic Multi-Correlator (SMC). A work about SMC can be get in [15]. The overlapping period is used in the SQM-metrics and depends on how fast the spoofer shifts the correlation function. We found, that a very slow shifting of the position (<0.01 m/s) is in general more difficult to detect, because the fluctuations caused by the Doppler difference are less often.

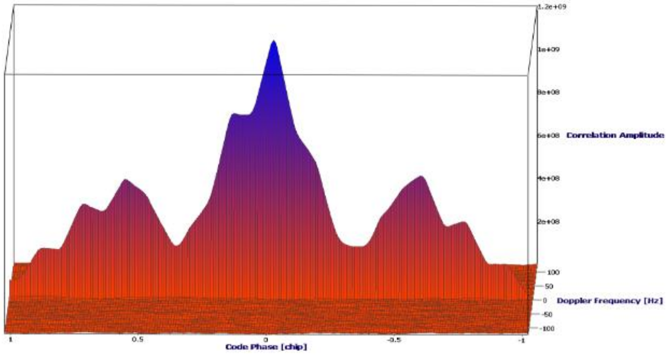


Figure 2: Correlation function of a Galileo E1B signal during the beginning of a spoofing attack, taken with IFEN SX3 software receiver

The spoofing process during the overlap period is a superposition of the authentic correlation function (CF), the spoofing correlation function and noise. Thus, the resulting CF in (1) is the sum of the authentic CF $R_a(\tau)$, the spoofer CF $R_s(t,\tau)$ and the noise $n(t,\tau)$, where τ denotes the code phase. Hereby, $R_s(t,\tau)$ is time dependent, because the spoofer shifts the correlation function with time in order to modify the navigation solution of the receiver. The noise $n(t, \tau)$ is also time dependent, since it depends on the thermal noise floor and the transmitted noise of the spoofer. An ideal spoofing attack should not change the noise floor, but which is not always straight-forward to achieve. Therefore, the C/N_0 most likely changes after the start of the attack. Depending on the power difference, the correlation function of the authentic signal can significantly worsen the quality of the spoofing signal due to the superposition.

$$R(\tau) = R_a(\tau) + R_s(t,\tau) + n(t,\tau) \tag{1}$$

The CF of the spoofer is given with:

$$R_s(t,\tau) = \alpha_s(t) R_a\big(\tau - \tau_s(t)\big) e^{i\cdot\varphi_s(t)} \tag{2}$$

$\tau - \tau_s(t)$ is the time dependent code phase difference from the spoofer to the authentic signal. For simplicity, equation (1) and (2) show the code correlation functions without the Doppler correlation. Thus, it should be noted that an induced velocity offset by the spoofer causes also a separation of the correlation functions in the Doppler domain. A start delay from the spoofer can cause a second peak in the code domain. For example the spoofer could have a start delay of several meters and shifts the code phase with 1 m/s away from the target. A start delay of 0 m is difficult to achieve, because the exact target coordinate has to be known. But even then due to the standard deviation of GNSS code measurements, which is on the meter level, a start delay on the meter level is common. However with simulations a start delay of 0 m is possible. $\varphi_s(t)$ describes the relative phase from the spoofer to the authentic signal, which is time dependent, when a position/time shifting is made. $\alpha_s(t)$ is the relative amplitude of the spoofing signal to the authentic signal, which is time dependent, when for example the power is increased slowly.

II.2 The investigated anti spoofing parameters

SQM metrics: Single Sided Ratio Metric (SRM), Delta Metric (DM), Double-Delta Metric (DDM), Ratio Metric (RM) and Threshold Fluctuation Metric (TFM)

In this subchapter we introduce briefly the well-known metrics, the SRM, the DM, the DDM and the TFM (treated in [9], most of them introduced in [20]). They are most often used in the literature. In the following metric descriptions, x is the correlator position, which is different for every correlator. In our case, we used 0.1 chip for x. C represents the correlator value at a certain correlator position and C_0 is the prompt correlator code phase. The DM, DDM and RM investigate changes in the shape of the correlation function between the left and right side of the correlation peak. The SRM and TFM just investigate fluctuations of the correlation function, which of course also occur when the peak shape is changing.

The Single Sided Ratio Metric is given by:

$$SRM = \frac{C_x}{C_0} \tag{3}$$

The Delta Metric is given in (4) and is also called symmetric ratio test. We used also 0.1 chip for x in this setup. This metric shall detect asymmetries between the left and right side of the CF, which occur during multipath and spoofing. Also like in all common metrics, the normalization by the prompt correlator is done to exclude effects of a changing total height of the whole CF. The reason for the height changes are for example variable receive/transmit antenna gains and C in the term C/N$_0$, scintillations or fading effects. Without the normalization the metrics would be falsified and no useful results would be possible. More details about the height changing effects can be get in [10].

The Delta Metric is given by:

$$DM = \frac{C_{-x} - C_{+x}}{C_0} \tag{4}$$

The Double-Delta metric is defined in the literature as the difference between 2 late-early correlator pairs, normalized by the prompt correlator. x was set to 0.1 chip and y to 0.05 chip.
:

$$DDM = \frac{(C_{-x} - C_{+x}) - (C_{-y} - C_{+y})}{C_0} \tag{5}$$

The Ratio Metric is defined as follows, where a is the slope of the correlation function (1 for GPS L1 C/A):

$$RM = \frac{C_{-x} + C_{+x}}{aC_0} \tag{6}$$

The correlator position x was also set to 0.1 chip for the RM.
The TFM is a multicorrelator metric consisting of 37 correlators, which investigates the mean over 37 moving standard deviation values of the Single Sided Ratio metrics compared with simulated noise only values [9].

Tracking parameters: Code Minus Carrier (CMC), C/N$_0$, Code rate of the replica (CRR), Doppler, Discriminator values, power of the I, Q and combined channel, DOP-values, number of PVT satellites, clock error, position accuracy and multiple-peaks in Doppler-delay maps

In this sub chapter the investigated anti spoofing parameters are explained with their advantages and limitations. In simulations, it turned out, that they are working better together than alone against spoofing. It depends on the spoofer settings like gain and delay, which parameters show significant jumps or standard deviation changes. In this paper, only the over the air attack with a specific spoofing setting is investigated, which all parameters could significantly detect.

CMC:
The CMC, which can also be considered as a spoofing detection parameter, is defined as the measured pseudorange minus the measured carrier phase. (7) and (8) represent the measured pseudorange P and phase θ. ρ is the error-free range, c is the speed

of light, *dt* the satellite clock error, *dT* the receiver clock error, *I* the ionospheric term, *T* the tropospheric term, λ the wavelength of the carrier, *N* the integer phase ambiguity and ε_θ and ε_{PR} the residual error factors of noise and multipath effects. X_{PR} and X_θ are the spoofing terms, since spoofing generally changes the phase and pseudorange.

$$P = \rho + c\ (\ dt_{sv}\ \text{-}dt_r) + T + I + \varepsilon_{PR} + X_{PR} \tag{7}$$

$$\theta = \rho + c\ (\ dt_{sv}\ \text{-}dt_r) + T - I + \lambda\ N + \varepsilon_\theta + X_\theta \tag{8}$$

Subtracting (8) from (7) gives the CMC. Since X_θ and ε_θ are much smaller than X_{PR} and respectively ε_{PR}, they can be neglected in the CMC. Our experiments showed surprisingly that *N* does not change during spoofing. If *N* would change, the parameter would still be suitable and would have even bigger jumps.

$$CMC = P - \theta = 2I - \lambda\ N + \varepsilon_{PR} + X_{PR} \tag{9}$$

The term λ *N* is the integer ambiguity that can be estimated in a differential measurement by the receiver. In a non-differential setting, *N* leads to a bias, which can be subtracted with software methods to get an unbiased result. This was the case in measurements with the IFEN SX3 receiver. Cycle slips did not occur in our experiments which is most likely due to the instant appearance of the spoofing signal. Also the term from the ionosphere leads to a bias, which can be subtracted. For jumps caused by spoofing *I* does not play a role, since *I* only changes slowly over time. When considering the standard deviation of the CMC as anti-spoofing parameter, which was not our detection goal here, only a short time interval of around 30 s should be taken to neglect ionosphere effects.

However a software approach could be to estimate *I* and subtract the over the time changing bias epoch by epoch. The remaining parts in the CMC are the multipath/noise term from the pseudorange ε_{PR} and the spoofing term X_{PR}. ε_{PR} is usually on the meter level and X_{PR} is the induced delay in meters. This delay can be less than the originally intended delay, because the authentic signal and the spoofing signal overlap and the combined correlation function is often times distorted, which leads to a not clear and generally also not exactly predictable prompt correlator tracking point. If the spoofer power is higher, the authentic signal can be neglected and the delay is similar than the intended one. All in all the CMC is suitable to detect spoofing attacks with an induced start delay. The delay should be at least on the meter level in multipath poor open sky GPS L1 C/A measurements in order to generate a clear jump. If there is no delay or a too small delay, the attack cannot be detected with this parameter. If a spoofing attack with a delay appears, the parameter is expected to rise significantly which then can exceed a certain fixed threshold. Generally this parameter cannot distinguish between multipath and spoofing. Therefore environments with strong multipath occurrence might be problematic if the start delay is low. But there could be an approach to look at different satellites and when all CMC parameters of the satellites rise at around the same time, it is very unlikely that it comes from multipath. A significantly changing C/N_0 can also change the standard deviation of the CMC, therefore the standard deviation of this parameter can also be used as a spoofing detection parameter. Sudden signal shading might be indistinguishable, but the look at many satellites still might lead to the distinguishing, since often times not all signals are shaded at the exact same time, where else spoofing occurs at the same time. The parameter is still easy to implement and it could support other anti-spoofing parameters in a concept of using many anti spoofing parameters in a receiver. A work about the investigation of the CMC against multipath can be found in [11].

C/N$_0$: The C/N_0 describes the carrier-to-noise-density ratio and is given by the ratio of the carrier power *C*, which arrives at the antenna, to the noise power density N_0 in the receiver, expressed in dB-Hz. The noise power density is given by $N_0=kT$, which is the receiver noise power per hertz, that can be written in terms of the Boltzmann constant *k* (in joules per kelvin) and the noise temperature *T* (in kelvin).

The bigger the C/N_0 the better the tracking quality of the receiver, since the correlation function gets more stable and defined. The spoofer often can adjust the C/N_0 with a signal generator. For the meaconing attack, there is no adjustment possible, since the signal is only amplified, which means that not only the signal but also also the noise is amplified. When the spoofer uses a much higher C/N_0 than the authentic signal and also a much higher signal power the authentic signal can be neglected. Then the combined signal has the C/N_0 of the spoofer. This leads to a parameter jump behavior, which can be detected.

If the C/N_0 of the spoofer is around equal to the authentic signal and the signal power of the spoofer only slightly higher, the C/N_0 will not change much. The C/N_0 can also decrease slightly in this case, fading effects occur more often in this case. If the C/N_0 is much weaker than the authentic signal, the spoofing attack can fail, since the spoofing signal might not be tracked at all. In general, the spoofer has to select carefully a proper signal power and C/N_0 in order to successfully spoof the target receiver. These parameters together with the delay are the most important parameters for the spoofer, which have to be estimated carefully before the attack.

If the spoofer would change the *C/N_0* slowly, it would be more difficult to distinguish it from a natural behaviour, for example multipath.

Since the *C/N_0* cannot exceed values over 55 dBHz for authentic signals, there is the possibility to identify values over 55 dBHz as spoofing, which is also easy to implement. This 55 dBHz threshold should therefore be implemented in every anti spoofing software.

Beside the 55 dBHz threshold, the *C/N_0* can also not be considered as standalone parameter because of the mentioned restrictions, but can support the other parameters.

CRR and discriminators:

The CRR is another candidate for spoofing detection. It is the speed of the replica, which is determined after a pass through the DLL. The DLL determines the code phase error and when the deviation is >0 compared to the last determined value it increases the speed of the replica and when the deviation is <0 it decreases the replica speed. In other words, the oscillator tries to follow the signal and compensate for dynamical changes for example from a user movement. When a sudden delay in case of a much higher spoofing signal is present, the oscillator changes the speed in a sudden abrupt behavior, which can lead to sudden jumps in this parameter. These jumps can be detected by threshold exceeding. The delay has to be bigger than normal deviations due to noise and multipath, since they also lead to replica speed changes. For the CRR also like for the CMC, the standard deviation can also be used. If the spoofer increases the *C/N_0*, the standard deviation of the CRR often times decreases which can also be detected. To avoid false alarms due to multipath, once again the many satellites study approach can be used. The CRR can be considered as additional anti spoofing parameter in a combination of a whole set of parameters, working under certain conditions. The code phase alignment error or also called the discriminator values of the DLL can also directly be used as anti-spoofing parameter and the same explanations are valid for this similar parameter. Furthermore the discriminator of the PLL can be used (deviations of the phase) as additional anti spoofing parameter, because in general the phase is changing, when the spoofing signal is arriving in the receiver. But since the phase due to a not predictable overlapping process can also change not significantly, this parameter can also not be used as a standalone parameter. It is nearly impossible to achieve a carrier phase coherent spoofing attack, due to the small wavelength and the required precise knowledge of the target antenna phase center. The chances to detect an attack are rising when the phase change of the spoofing signal exceeds the PLL bandwidth significantly, because the PLL lock can be lost in this case which is conspicious. The standard deviation of the discriminator values can also be used as detection approach due to the same explanation than for the CMC and CRR. Also, the FLL discriminator can be used.

Doppler:

The Doppler value changes when the spoofer tries to shift the position away with a certain speed or acceleration. A Doppler-based detection can only be deployed, if the own dynamics can be predicted with a suitable dynamic model. In general, an instantaneous Doppler offset can lead to a jump and a sudden acceleration to a kink-like curve. The slower the speed or acceleration the harder to detect. An acceleration always flattens the Doppler curve and avoids jumps. But the kink is in general detectable then. The Doppler is not suitable as standalone parameter because of the restriction that it can only detect well higher speeds without acceleration. The standard deviation can also be used here (same explanation as before).

AGC and Power I/Q:

Since the spoofing signal requires a higher signal power than the authentic signal in order to get tracked, the power level in the frontend increases when the spoofing signal arrives. The AGC adjusts the power level to ensure that the Analog Digital Converter (ADC) is not getting saturated. Therefore, the AGC decreases the gain when the higher spoofing signal arrives. Based on the fact that a GNSS receiver samples just the noise floor, the AGC should remain constant in a typical receiver-antenna setup. Thus, a change in the AGC values can only result from a change in the Radio Frequency (RF) setup or from interferences. However, a low spoofing signal power compared to the authentic signal of only some dB might also be difficult to detect, as it also depends on the sensitivity of the AGC. A drawback of the AGC is, that many receivers, especially low-cost receivers, do not provide the AGC output. Another drawback with the AGC parameter is, that spoofing cannot be directly distinguished from interference or intended jamming. Therefore, the false alarm rate might be too high in modern urban regions where interference can occur all the time. Therefore, this parameter can also serve only as an additional anti-spoofing parameter in a setup of several different anti spoofing parameters.

The power which is left in the I-channel after the successful lock of the PLL and after the code and carrier wipe-off contains the data bits with an amplitude proportional to the square of the amount of power. Therefore, the power can be determined with the I-channel or also with the Q-channel. The power normally rises when the spoofing signal arrives, but decreases again when the AGC decreases the power level. It depends on the speed of the AGC, how fast the power level is adjusted. For our receiver (IFEN SX3) the I and Q channels could be used against spoofing. When the gain of the spoofing signal is only some dB it can be difficult to exceed a certain anti-spoofing threshold. Furthermore, for a slowly increasing spoofing signal power, the I/Q channel power detector can fail, because the power in the I and Q channel does not show a clear jump behavior. Just a slow increase of a value is difficult to mathematically handle, because it can also appear under normal circumstances.

Clock error:

The receiver clock error, also known as receiver clock bias, can also be taken as anti-spoofing parameter. The receiver clock error and receiver clock drift describe the offset of the receiver time to the GNSS time. The receiver clock error is used to correct the internal receiver time in order to obtain the GNSS system time. In general, the true GNSS system time cannot jump forward or backward, and any jump could be detected. Hereby, a signal generator based spoofer would be capable to shift the time into the past and future, whereas a meaconing or record and replay attack will always shift the time into the past.

The receiver clock is driven by an internal oscillator. Receivers typically use cheap Temperature Controlled Oscillators (TCXO) and clocks of higher quality are usually not required, because the receiver can align the clock error each epoch when solving for the navigation solution. Even cheap clocks like a TCXO have a reasonably good frequency stability over several seconds, and thus jumps caused by an imperfect aligned spoofing attack or meaconing and record replay attacks can be detected.

Meaconing attacks are based on a repeater, which receive, amplify and retransmit all received GNSS signals, typically from a single spot. Thus, all retransmitted GNSS signals have the same delay, which results in a shift (jump) of the clock error, if the receiver was spoofed successfully. With a meaconing attack, the magnitude of the induced delay is in the order of the distance between the meaconer transmission antenna and receiver antenna, plus the internal hardware delays of the meaconer.

The record and replay attack most likely will transmit recorded signals from several hours, days, weeks, month or years in the past. In such a case, the satellite constellation is most likely not the same. Furthermore, the GNSS time will jump significantly in to the past (theoretically also into the future, if the recorded signal was generated with a GNSS simulator). In such scenarios, the clock error and GNSS time will show a significant and detectable jump.

It should be noted, that a highly sophisticated (time) spoofing attack with multiple GNSS antennas requires that all transmission spots are timely synchronized. The clock error can give a good indication of a present spoofing attack, nevertheless it is recommended to use it in an assemble of spoofing detection parameters to achieve a robust detection in an anti-spoofing software.

PVT losses/DOP values:

The number of satellites, used for a PVT solution, can decrease during a spoofing attack, because some pseudoranges might have a lower quality to the overlapping process of spoofing and authentic signal. The number of tracked satellites can differ, if the spoofer uses other satellites than the ones in the authentic one. In this case also the DOP values can change, which can be detected. Especially in the Record and Replay attack generally another set of satellites than the one from the victim receiver is used.

Position accuracy:

The pseudorange quality will most likely decrease significantly, when the spoofing attack starts and when the spoofing and authentic signal are overlapping. Especially in the first seconds after the spoofing signal arrives at the receiver, the tracking gets confused due to distorted correlation functions. When the spoofer tries to shift the position away, the pseudorange standard remains significantly increased, as long as the correlation functions overlap. Once the spoofed position is that far apart from the true position, such that the correlation functions do not overlap anymore, the fading effects are gone and the pseudorange standard deviation settles back. The noise on the pseudorange measurements directly affects the standard deviation of the position, since they are taken for its calculation. Therefore, the position noise standard deviation can also be taken as anti-spoofing parameter, if the receiver is operated in clear open sky and known conditions.

Multiple peaks in Doppler-Delay maps:

A further detection candidate is the checking for double or multiple peaks in the acquisition and tracking correlation function. Two or several peaks would indicate the presence of one or several spoofing signal. Typical Application Specific Integrated Circuid (ASIC) or Field Programmable Gate Array (FPGA) based GNSS receivers do typically not have the processing power to evaluate massive correlation points. Software based GNSS receivers can benefit from the high processing power on Central Processing Units (CPU) or Graphic Processing Units (GPU) to calculate massive correlators in a Doppler-delay map. This can be efficiently realized using Fast Fourier Transform (FFT) based acquisition techniques or using a Synthetic Multi-Correlator (SMC) applied to tracking post-correlation values. Doppler-delay maps allow to observe the correlation domain in the code-phase and Doppler direction, as well as to visualize authentic and not-authentic correlation functions.

Hereby, a spoofer signal leads to a second bigger correlation function peak, which is in the beginning of the sophisticated well aligned attack close to the authentic correlation function. If the spoofer is not perfectly aligned or a meaconing attack is present, a second correlation function immediately appears, which can be detected with superior robustness. Even, a well aligned sophisticated spoofing attack could be detected, if the spoofer starts shifting the position away, because the correlation peaks move apart from each other. The separation will be visible in the code phase and Doppler domain. If the receiver was spoofed successfully, the spoofing signal correlation peak remains at the prompt correlator position, and the authentic correlation seems to drift away in the Doppler-delay map. The evaluation of the Doppler-delay map is computational intensive, and a limit in the code-phase and Doppler might be introduced in order to achieve a real-time monitoring. If enough processing power is available, the full code-periods and a very large Doppler space can be monitored.

The FFT based Doppler-delay map from the acquisition typically (cold start) evaluates the full code period and a Doppler of several kHz. The resolution of the map depends on the sample rate and the processing performance, if a real-time evaluation is targeted. Since the correlation peaks are not only in the code phase domain but also in the Doppler, a significant Doppler change (spoofing of velocity and/or clock drift) can also lead to a separated peak in the Doppler region. Low spoofer speeds are hardly separable, since the Doppler is only roughly estimated at the acquisition stage. The double-peak methods are easy to medium to implement. Only spoofers that shift the correlation peak significantly can be detected, since otherwise the peaks are not separable. When the spoofer shifts the position away, after some point in time, the peaks can be separated, which depends on the spoofer shifting speed. If the shifting process is low, it can take a longer time till a spoofing attack can be detected. Another restriction is, that when the spoofer uses a higher gain, the authentic correlation peak can be negligible small and not be distinguished well from noise. But the multi-peak parameters can very well support an anti-spoofing software.

The acquisition peak method can detect higher code and Doppler offsets, is however not so sensitive than the tracking peak method which estimates the code phase and Doppler more exactly. Also, the receiver software has to be changed that an ongoing acquisition reoccurs, even when a satellite is tracked. This can severely increase the processing load since the acquisition requires generally the most computing effort in a receiver compared to other receiver stages like tracking or PVT calculation modules. An advantage of the multi peak method is, that code phase delays bigger than a chip can be detected, which SQM metrics cannot afford. Those big code phase delays can occur for example for a spoofing attack, that shifts the correlation function first with a Doppler to the victim peak (approximation attack). Then the attack could be detected even before the correlation peaks overlap. Furthermore, the method allows to detect any spoofing attempt, even if the spoofer was not perfectly in sync. Note, that the spoofer signal can only be tracked if an overlap occurs. [12] is a work which also suggests the acquisition multiple peak detection.

II.3 The signal generator LOKI-Spoofer and the measurement setup

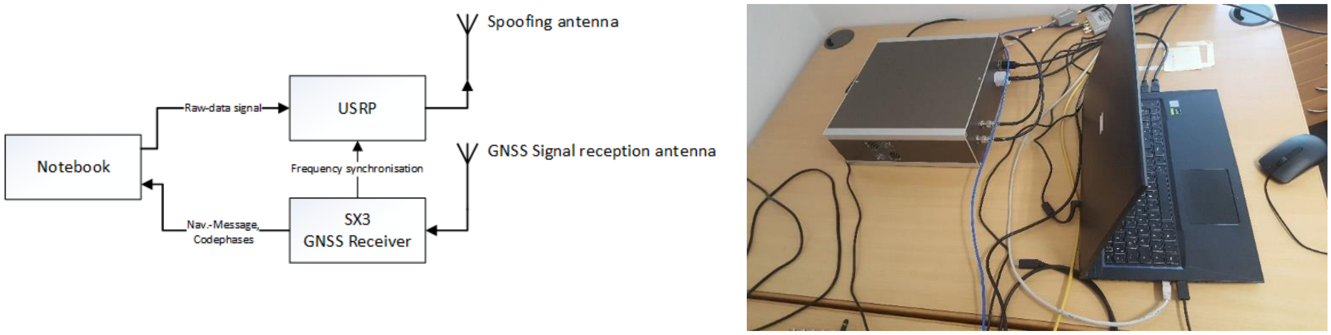


Figure 3: Left: Internal structure of the LOKI spoofer, right: LOKI spoofer (box) with notebook

The used spoofing device, the LOKI-Spoofer [14], is able to generate Galileo E1 B/C and GPS L1 C/A signals from currently visible satellites with either 2.5 or 5 MHz sample bandwidth (2.5 MHz used in our setup). In Figure 3 we see on the left the schematic setup of the LOKI spoofer experiment and on the right the spoofing device with the notebook for operating. In the spoofing device an SX3 receiver extracts the complete navigation message with almanac and determines the GNSS time for steering the USRP's oscillator. With the navigation message the signal at the victim's antenna is estimated and the baseband signal is send to the USRP, where it is upconverted to the L1 carrier frequency and finally transmitted over the air.

The spoofer is able to adapt the RF output gain. It is important to find a suitable setting for the RF gain so that the spoofed signal has a slightly higher power than the true signal. On the one side spoofing with too much power would jam the victim receiver which can be easily detected and on the other side spoofing with less power than the genuine signal might not affect the receiver's tracking loops. An RF output hardware delay can also be set in the LOKI configuration, which is necessary to account for additional signal delays such as propagation delays of RF equipment and cables in the path between RF output and antenna or in our case combiner. The minimum step width of the hardware delay setting is 100 ns which limits the accuracy of the code phase alignment between counterfeit and real signal. A work about the development of a portable GPS spoofer can be found in [18].

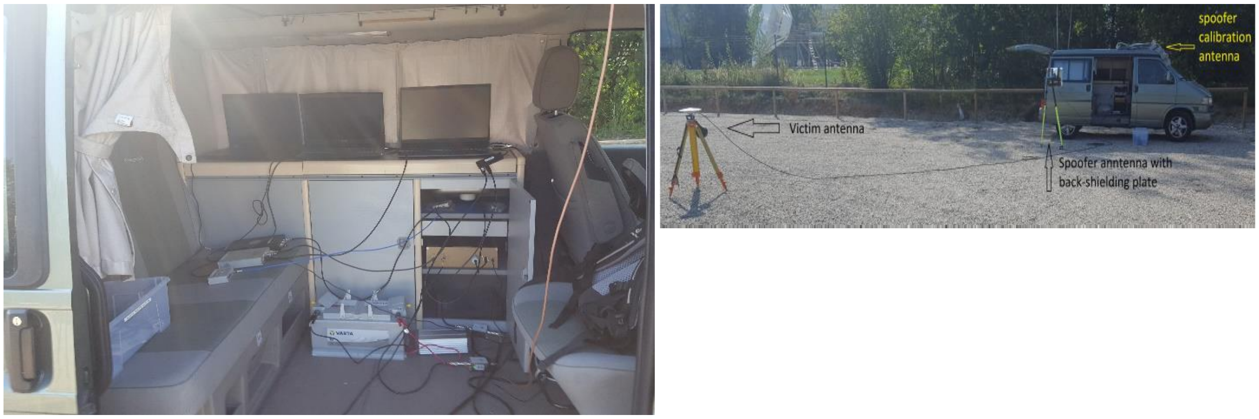


Figure 4: On the left the inner of the measurement bus with the three receivers on the back seat (in front U-Blox M8T, in the middle the IFEN Sx3 and in the background the Septentrio PolaRx5TR). In the drawers the LOKI-spoofer. On the bottom the power supply battery with a power converter. On the right the victim antenna (front) and spoofer antenna (back).

III. RESULTS

In the following, the results from the over the air spoofing are presented for three receivers. The behavior of the spoofing is explained with tracking parameters and SQM metrics. There were 4 characteristic spoofing phases. The first is before the attack, where the spoofer was switched off and only the authentic signals were tracked. In the second phase, the so-called static spoofing phase the spoofer was switched on but no position shift was induced. In the third phase, an accelerated position shift (0.1 m/s²) was induced with a changing Doppler value. In the fourth phase a constant position shift was performed, which started when the speed of 25 m/s was reached. Three receivers were spoofed simultaneously, the low cost U-Blox M8T (<500$), the Septentrio PolaRx5TR (>10000$) and the IFEN SX3 (>10000$). The over the air spoofing attack was performed on an open sky parking place. The set spoofing trajectory was from IABG (Ottobrunn, Germany) to Starnberg, Germany.

III.1 U-Blox M8T

The U-Blox M8T was not studied in detail, but the position could be successfully shifted away (Figure 5). The position shift was not so smooth and in the range of several hundred meters instead of thousands of meters as for the other investigated receivers. This might be due to the internal Kalman filter in this timing-receiver.

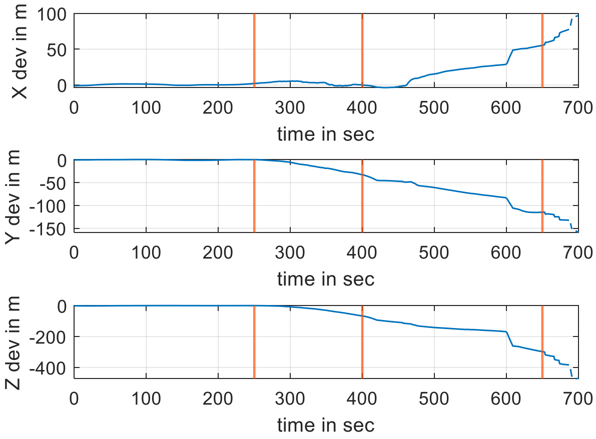


Figure 5: Deviation between starting position and U-Blox M8T receiver position in X, Y and Z direction (ECEF)

III.2 Septentrio PolaRx5TR

The Septentrio receiver was set to track all L1 signals, GPS L1 C/A, Galileo E1B/C, GLONASS L1 and Beidou L1. The spoofing device can only generate GPS L1 C/A and Galileo E1B. The attack was successful, since the position could be shifted kilometers away, but the standard deviation of the position was quite high.

The spoofing attack started at 14:13 with a first static spoofing phase (first orange line), where the position is not shifted away. At 14:15 the position was shifted away (second orange line) with an acceleration of 0.1 m/s² till the end speed of 25 m/s is reached at 14:19:10 (third orange line) and kept constant then. In Figure 6 on the left side the position components are shown in East, North and Up direction (ENU coordinates). All three coordinate components showed more or less the accelerated drift, although with some noisy behaviour, especially the North component. More outliers/deviations occurred after 14:19, especially for the y-component, when the acceleration was set to zero and the velocity was kept constant. The set end velocity was 25 m/s, which however was not reached here. It seems, that an immediate drop of the acceleration can worsen the tracking quality. The total deviation was in the end around 5 km for the East, 4 km for the North and 2.5 km for the Up component. This shows that the target receiver was fooled kilometres away from the original position, although the target antenna was not shifted. On the right side in Figure 6 the C/N_0 for the GPS L1 C/A signals is shown. In the static spoofing phase the deviation was very high compared to before the attack and when the position was shifted. When the attack started, the C/N_0 of most of the satellites dropped slightly. Afterwards, the fluctuations started with a slight delay of around 25 s, which is most likely the point in time when the receiver tracks the spoofing signals (could be observed for the SX3 receiver, see below). The reason for the fluctuations generally lies in the distorted correlation function, the spoofing signal with the code phase delay and higher amplitude disturbs the shape of the authentic correlation peak. The LOKI compensates for the Doppler caused by the satellite motion and clock, but the satellite orbit and clock modeling, spoofer clock prediction and possible changing reflection points cannot to be known perfectly, which cause fading effects. When the spoofer starts the position shifting, the fading effects more or less disappeared but still outlier phases remained. We assume, that the high Doppler of the spoofer leads to the effect, that a relative phase offset between authentic and spoofing signal changes faster and therefore fading effects cannot be so distinct. When the acceleration stopped, the fluctuations increased for 2 out of 9 satellites. This also might explain why the position components deviated more after this point in time.

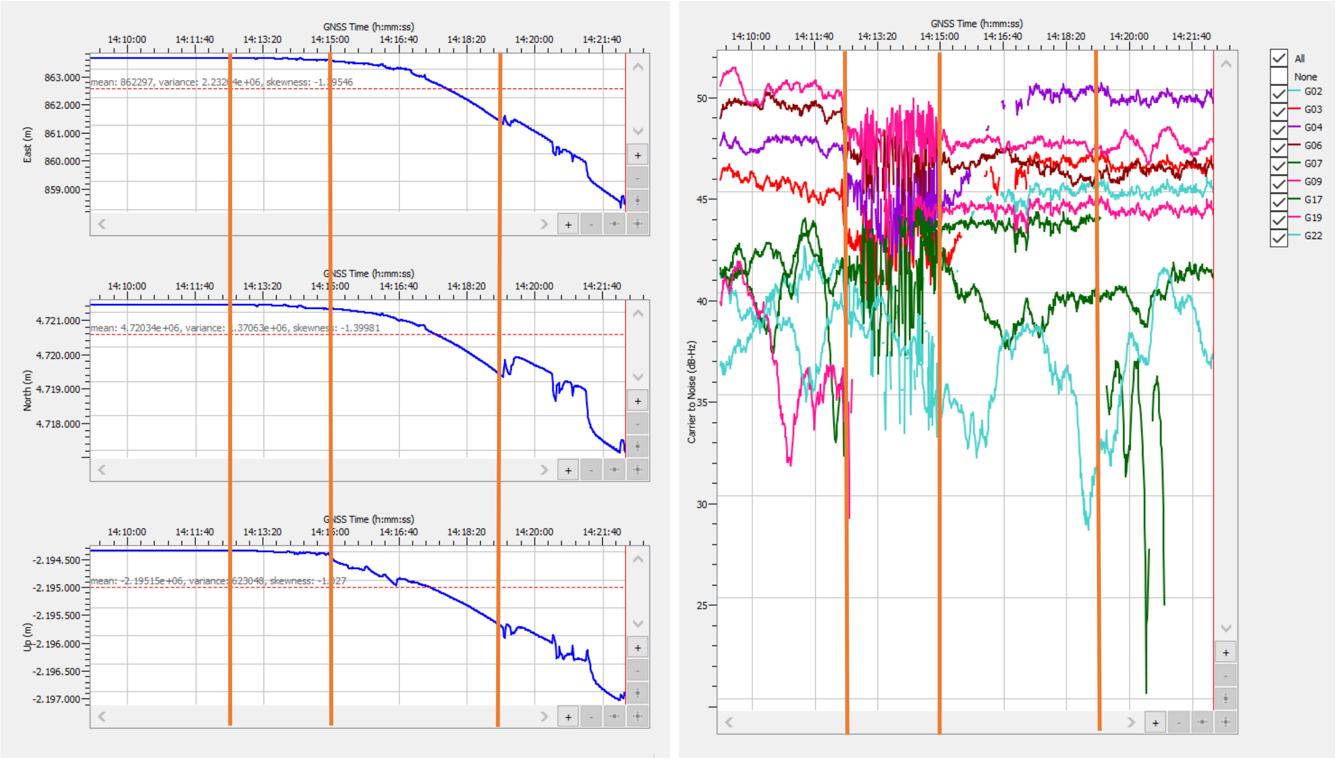


Figure 6: Septentrio PolaRx5TR, on the left side East/North and Up coordinate [m] over time, on the right side C/N₀ [dBHz] of the GPS L1 C/A satellites over time

Figure 7 shows the clock error (clock bias) on the left side. Since no time spoofing was performed, the clock-drift which started after the beginning of the attack was surprising. We could not identify the reason, but it could come from a not perfect estimation of the signal parameters in the spoofing device. On the right side the satellites in tracking (upper plot) and the satellites taken for PVT solution (lower plot) are shown. The number of satellites in tracking was not different on average than before the attack, also the number of satellites taken for PVT was quite similar, slightly less in the static phase. A slight increased fluctuation of the number of satellites in PVT occurred during the static spoofing phase, a change from 32 to 34 satellites changed here rapidly over time. After the position started to shift, this fluctuation again decreased. It is supposed that a few satellites and therefore pseudoranges were not of good quality and therefore were sometimes taken for PVT and sometimes not.

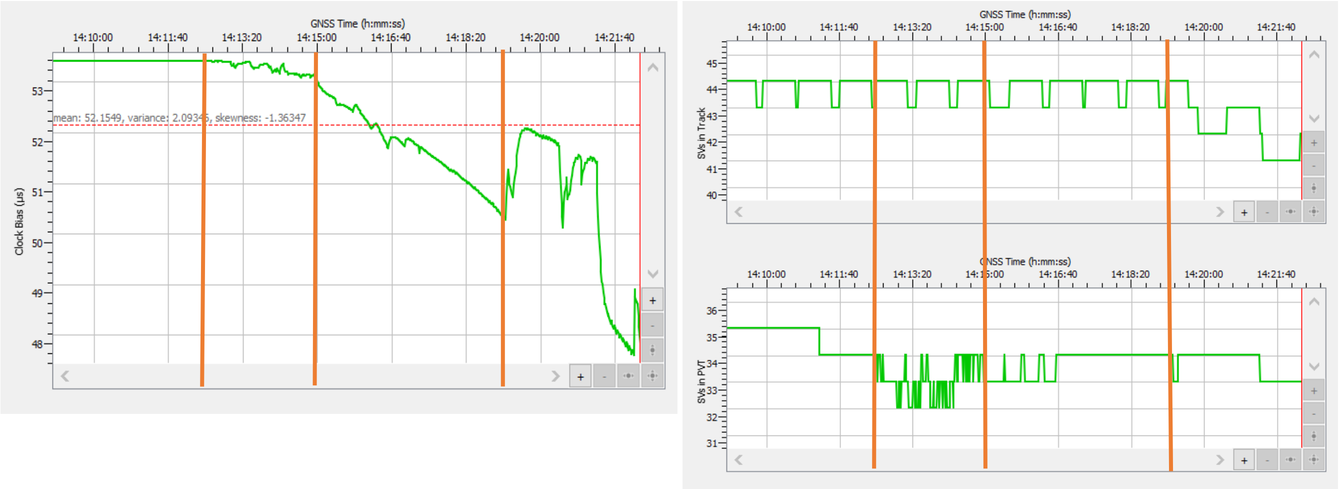


Figure 7: Septentrio PolaRx5TR, on the left side clock bias [µs] over time, on the right side upper plot satellites in tracking over time, lower plot number of satellites used for PVT over time

Figure 8 shows the standard deviation of the position components (ECEF x, y, z) on the left side. The standard deviation for the x and y component clearly rised after around 25 s after the spoofing attack started with a higher fluctuation than before the attack (around 1 m more). The reason for the increase is the correlation function distortion, which leads to imprecise tracking and pseudorange computation. Since the pseudoranges are taken for PVT solution, the standard deviation of the position also increases. When the position started to shift, the fluctuations decreased, but still the standard deviation values were high. The reason is because the correlation function gets more stable. After around 100 s after the shift, the standard deviation decreased to quite similar values than before the attack with a few outliers occurring after the acceleration stopped at 14:19 at least for the x and z component. The Z-component showed also a higher standard deviation during the static phase, but not so distinct and the decrease to values before the attack occurred much earlier already in the end of the static phase. Noticeable was also, that some higher standard deviation values also occurred for the z-component before the attack, which might be due to multipath.

On the right plot, the velocity components in East, North and Up- direction are shown. In the static phase a few outliers occurred, especially for the North-component. The reason is like for the position standard deviation the distorted correlation function. However, the velocity components are more stable than the position components in the static phase. At 14:19 the velocity changes to a more or less constant value.

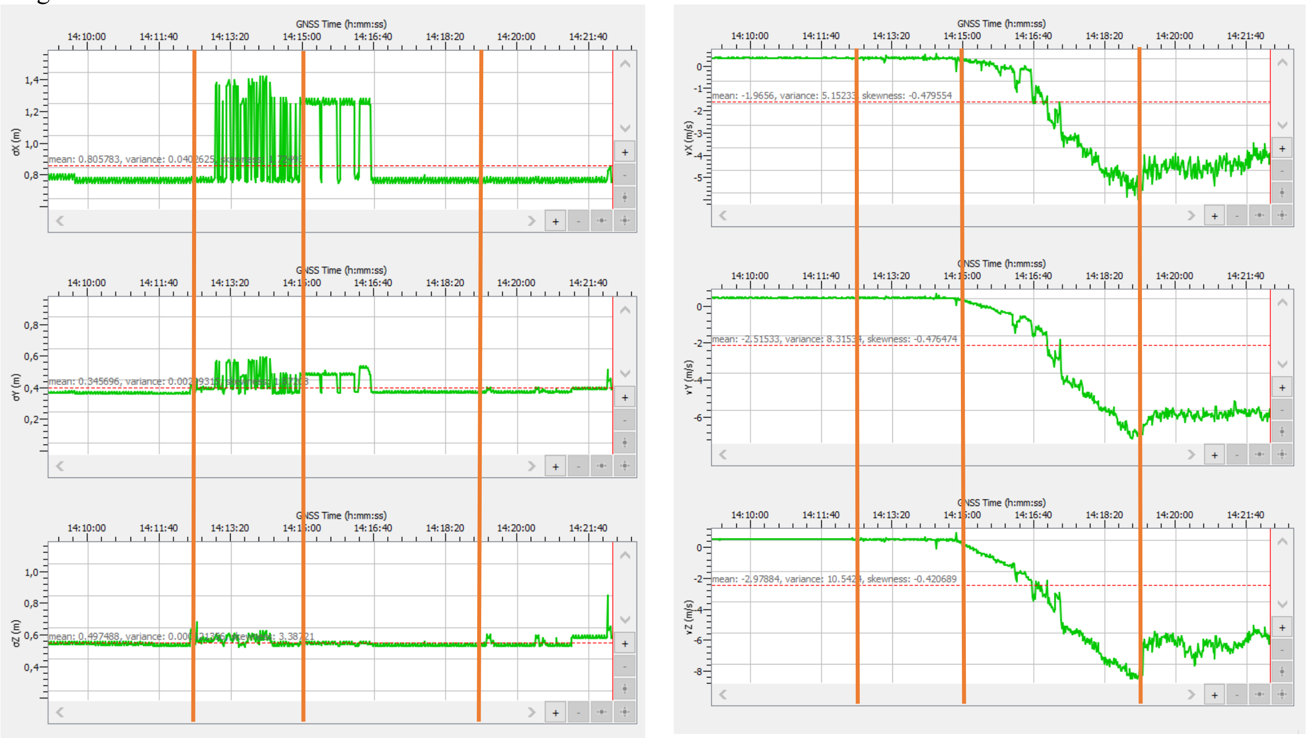


Figure 8: Septentrio PolaRx5TR, on the left side standard deviation of the X, Y and Z component (Earth Centered Earth Fixed (ECEF) coordinate system). On the right side velocity components [m/s] in X, Y and Z direction.

Also all the DOP values (PDOP, GDOP, TDOP, HDOP) showed an increase and more varying behavior in the static spoofing phase (Figure 9, shown for PDOP) compared to before the attack. This is consistent to the number of satellites used for PVT, which also varied more in the static phase. The behaviour during the position shift was not significantly different than before the attack. On the left side of Figure 9 the sky plot is shown during the static spoofing phase, which shows a good satellite distribution of the GPS satellites. Figure 10 shows the latitude/longitude plot, where on the right side the point cloud from the phase before the attack and during the static spoofing phase is shown. Towards the left side, the trajectory is shown, caused by the spoofing. The trajectory has a high deviation but the receiver could be spoofed kilometres away successfully. We found out, that the deviation increased when the acceleration stopped and a constant speed of 25 m/s was used.

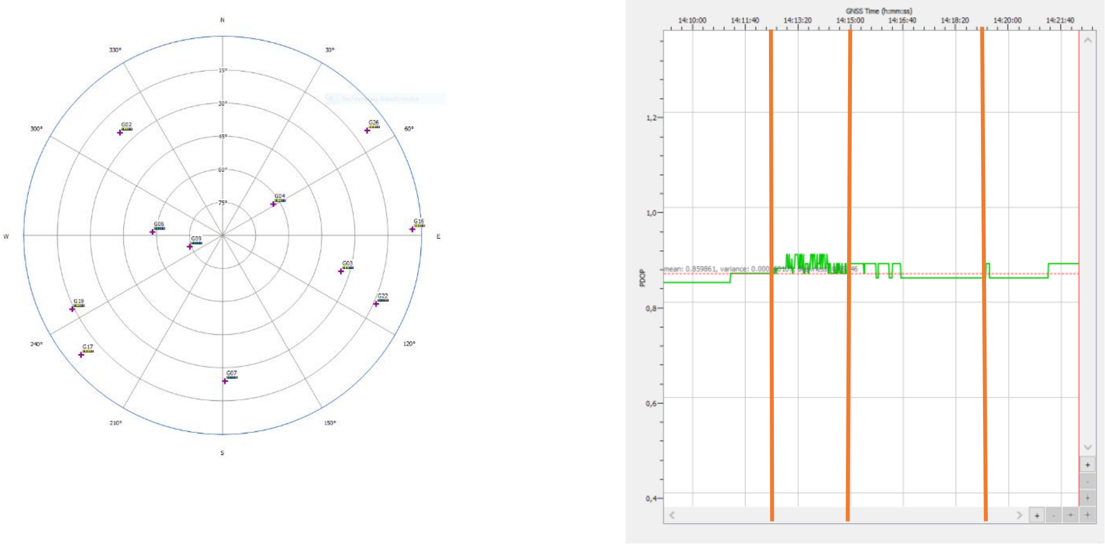


Figure 9: Septentrio PolaRx5TR, on the left side sky plot of the GPS satellites, on the right side PDOP values over time

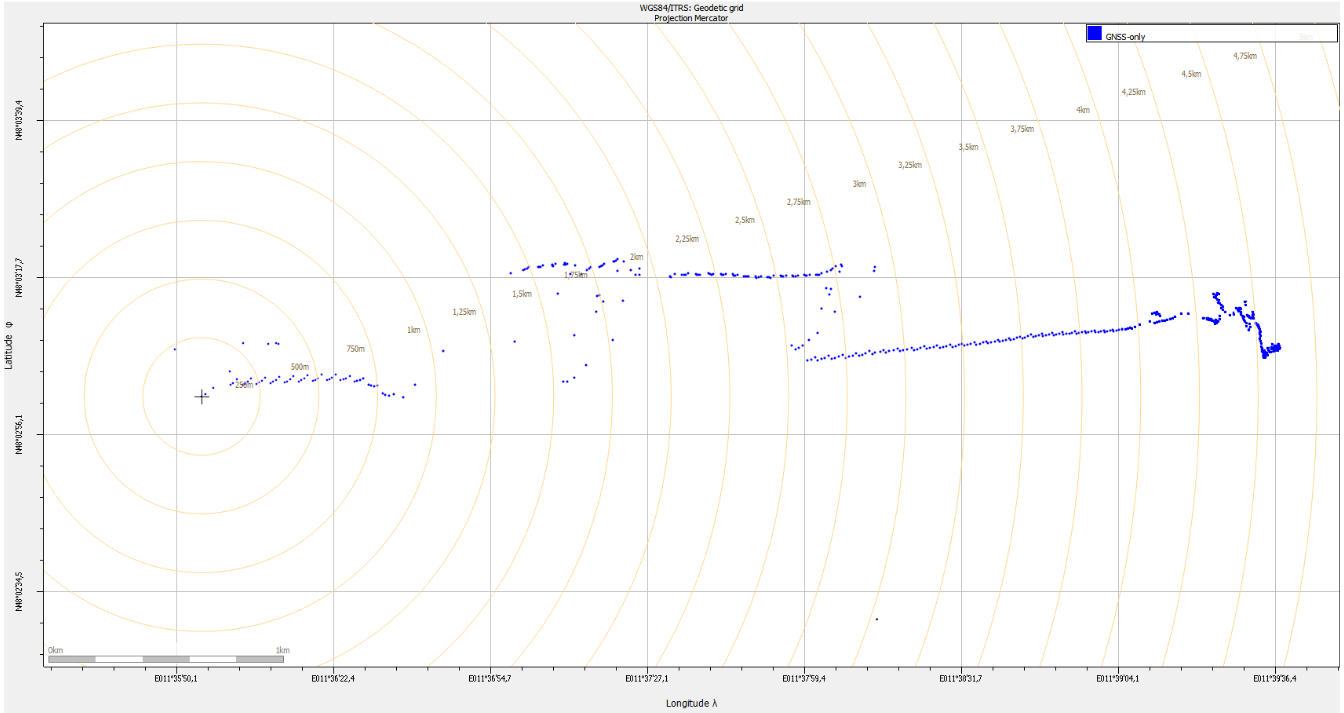


Figure 10: Latitude/Longitude plot. On the right side the point cloud of the static spoofing phase and phase before the attack is shown. The trajectory went towards the left side, but with temporary high deviations

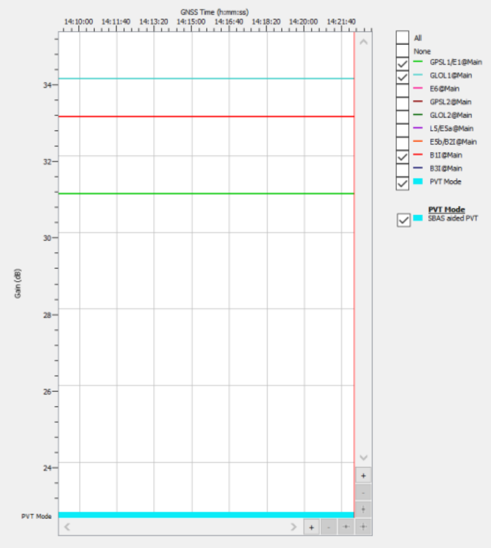


Figure 11: Frontend gain values for GPS L1 C/A+Galileo E1 (green), Beidou L1 (red) and GLONASS l1 (blue). No changes are seen over the whole time.

The frontend gain (AGC values) can be distinguished from GPS L1 C/A+Galileo E1, GLONASS L1 and Beidou L1 in the Septentrio receiver. There were no changes over time (Figure 11), which was a bit unexpected and shows, that the AGC not necessarily changes during a spoofing attack. The spoofer power was set to be 3 dB higher than the authentic signals. The result might have been different, when also Beidou and GLONASS signals would have been transmitted, because then more energy would arrive at the antenna.

There was an unsolved question at the time of writing. First, it was unexpected that the receiver can be spoofed successfully, even if not all satellite systems have been spoofed. In this experiment, only the GPS L1 C/A and Galileo E1B/C satellites are spoofed, while the Beidou L1 and GLONASS L1 satellites were not existing in the spoofing signal. The authentic GLONASS and Beidou signals were still tracked and taken for PVT solution during the attack, but still the position was shifted kilometres away. It was clearly visible, that the GPS and Galileo signals changed the behaviour during the attack and were therefore affected from spoofing, while the GLONASS and Beidou signals remained unaffected. One idea could be, that the receiver takes the GPS and/or Galileo satellites with a higher weight in a Kalman filter. Further experiments have to be done to also check, what happens when other signal bands like the L5 are additionally tracked. This result also shows, that spoofing is potentially easier to achieve, since the spoofer does not necessarily need to generate all systems, at least shown for this specific receiver. Of course, the result might be different for other receivers.

III.3 IFEN SX3/MuSNAT

The IFEN SX3 frontend recorded the IF samples during the attack. The samples were later analysed in the MuSNAT software receiver [13]. The spoofing attack in terms of position shifting was successful. Here, GPS L1 C/A and Galileo E1B/C were taken for PVT with SPP solution. The orange bars in the following plots show as before for the Septentrio receiver the start of the spoofing attack, the start of the accelerated position shift and the transition from an accelerated to a linear position shift. In Figure 12 the CMC is shown for the GPS L1 C/A satellites. After the start of the attack, the CMC dropped for one satellite immediately and after around 30 s for all the other satellites at around the same time. The jumps had around the same height and illustrates the good detection ability of this parameter for the used spoofer settings. Clear jumps are suitable for detection with threshold exceeding methods. The standard deviation was high in the static spoofing phase and as low as before the attack in the movement phase. The reason lies in the Code pseudorange fluctuations, which were higher in the static spoofing phase due to the higher correlation function fluctuations due to more distinct fading effects between authentic and spoofing signal. In Figure 13 the *C/N_0* is shown. The behaviour is quite similar than for the CMC, only that the jumps are not so high and that the fluctuations lasted a bit longer after the start of the position shift. After around 420 s, the correlation functions begin to separate depending on the elevation angle of the satellite. When the separation is done, the fading effects decrease and the fluctuation of the *C/N_0* as well. Of course, multipath can still occur.

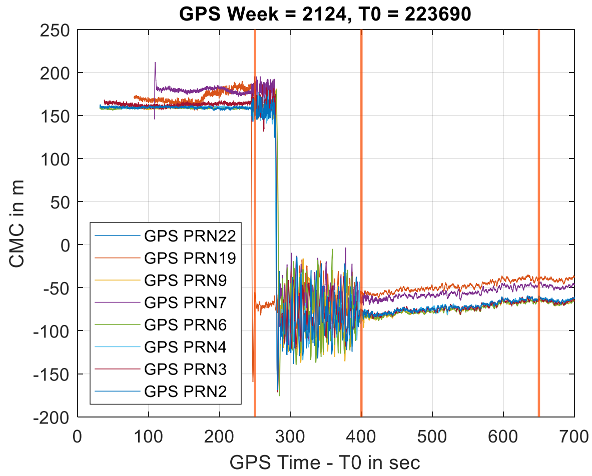


Figure 12: Code-minus-Carrier (CMC) over time

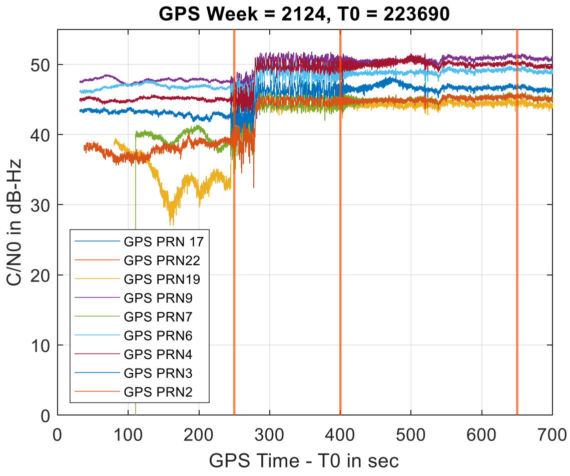


Figure 13: C/N0 over time

Figure 14 shows the CRR value for the GPS L1 C/A satellites. After the start of the attack, the standard deviation of the CRR increased immediately after the spoofing start at around the same time for all satellites, which can be used as a spoofing detection. After around 25 s (at 275 s) the deviation goes a bit down, but was still higher than before the attack. It seems, that the NCO tries to adapt the replica right after the attack and after some time when the spoofing signal is tracked, this adapting process gets more stable. PRN 19 also showed high fluctuations before the attack, it is assumed due to multipath. After around 430 s the deviations go completely down to a level even smaller than before the attack for at least 5 satellites. We assume, this is because the correlation peaks are going into separation at this time. 2 satellites (PRN2, PRN3) still showed deviations till 550 s, which might be due to the low elevation angle, leading to more multipath.

The discriminator values for PRN 6 are shown as an example in Figure 15 for the DLL, PLL and FLL as well as the Doppler. The FLL discriminator only showed a slight deviation after the start of the attack while the DLL and PLL discriminators showed a clear deviation, which illustrates the detection ability potential. The Doppler shows a small kink-behavior when the position starts to shift at 400 s and again a slight change when the acceleration goes into a linear shift at 650 s. Therefore, also the Doppler turned out as a detection parameter, at least for a static scenario.

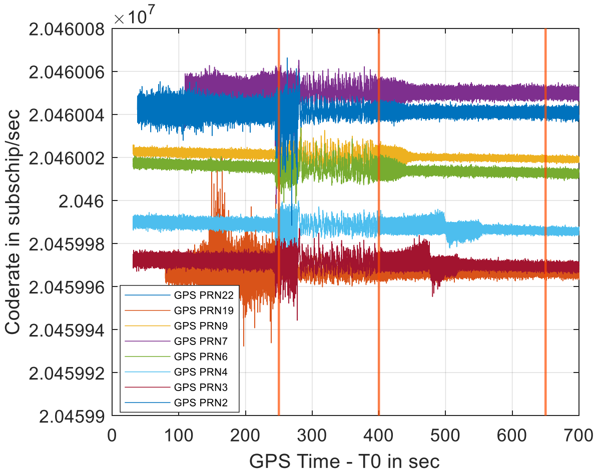


Figure 14: CRR over time

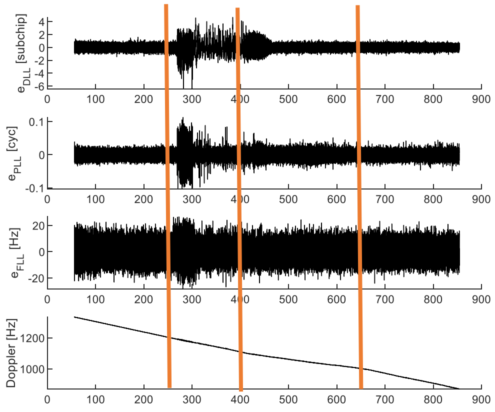


Figure 15: Discriminator values of DLL, PLL and FLL and Doppler values over time

Figure 16 and Figure 17 show the I and Q channel values for all GPS satellites over time. After the start of the attack, the Q-channel values showed a higher deviation immediately for all satellites while for the I-channel the deviation increased immediately for one satellite and for the others after 25 s delay at around 275 s. Both, I and Q channel turned out to be a suitable detection parameter, while for example the AGC for the Septentrio receiver was not a suitable detection parameter.

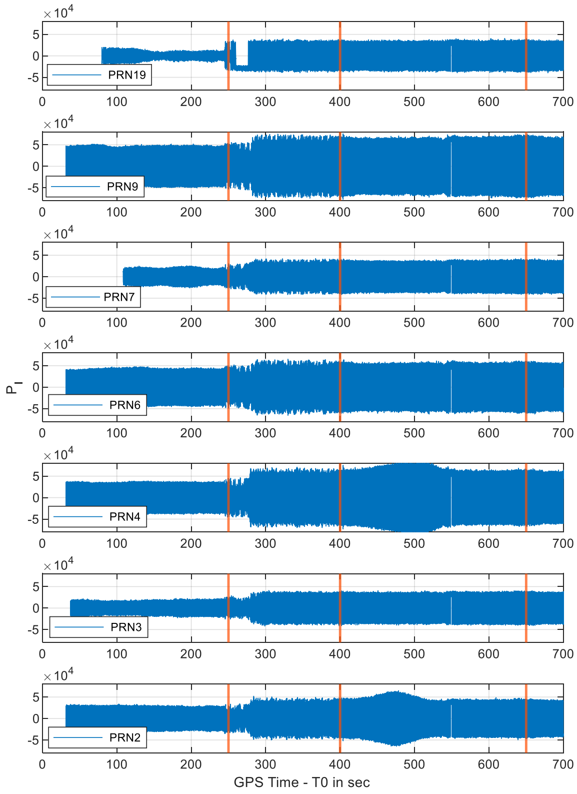


Figure 16: I- channel values for all GPS satellites over time

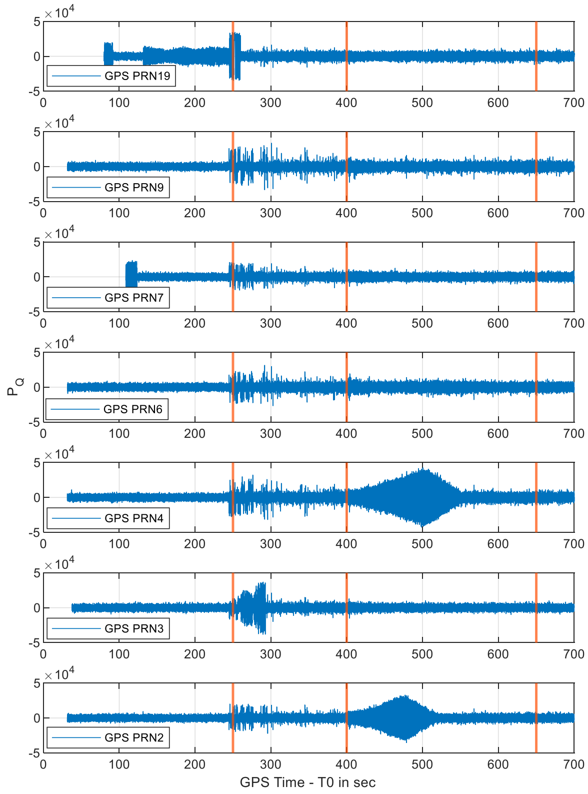
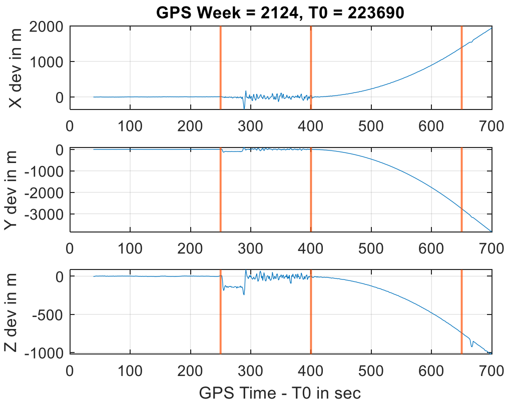


Figure 17: Q- channel values for all GPS satellites over time



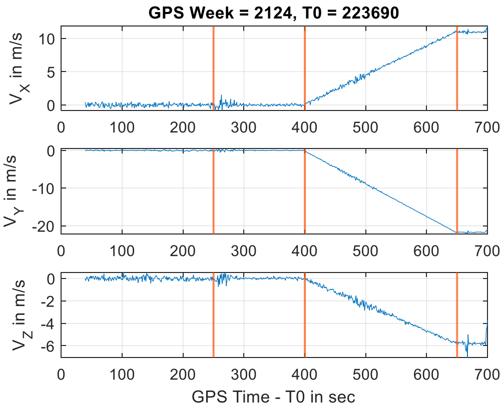


Figure 18: Deviation between starting position and receiver position in X, Y and Z direction (ECEF)

Figure 19: Velocity components in x, y and z direction

Figure 18 shows the ECEF position components in X, Y and Z direction. Higher fluctuations also occurred in the static spoofing phase. The accelerated movement is more distinct than for the Septentrio receiver. Figure 19 shows the velocity components, which are also more distinct than for the Septentrio receiver. The transition to the linear speed phase can be seen clearly and the end velocity of around 25 m/s was also shown. The position and velocity components fluctuate more in the static spoofing phase and show a very smooth unnoisy behaviour during the shift phase. The fluctuations for the position components started after 25 s after the spoofing start, when the spoofing signal was tracked for all satellites. The velocity components showed also a fluctuation directly after the spoofing start which was more stable after 25 s. Further research is needed to understand this behaviour.

The correlation peaks from the authentic and spoofing signal can be seen for the GPS L1 C/A in Figure 20, Figure 21 and Figure 22. Before the attack there is only one peak visible from the authentic signal. During the static spoofing phase (Figure 21) two correlation peaks are visible quite close to each other with a code phase difference of around 250 m. In Figure 22 the peaks are nearly separated during the beginning of the position shift. They are completely separated in Figure 23.

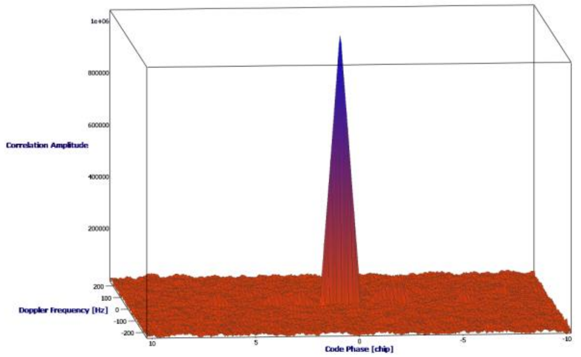


Figure 20: Multicorrelator-Plot of GPS PRN 6 before spoofing. Only the authentic signal is present.

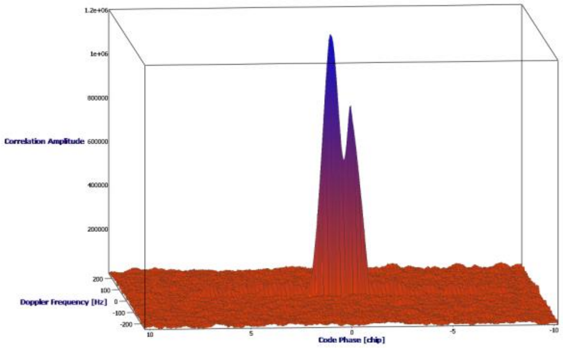


Figure 21: Multicorrelator-Plot of GPS PRN6 during the static spoofing phase. Both correlation peaks are close to each other. The higher peak which is more flattened corresponds to the spoofing signal.

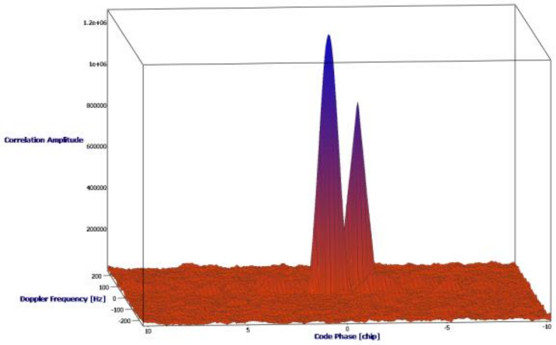


Figure 22: Multicorrelator-Plot of GPS PRN 6 during the time the spoofer shifts the position away. Both peaks are clearly separated in code-phase and Doppler frequency from each other.

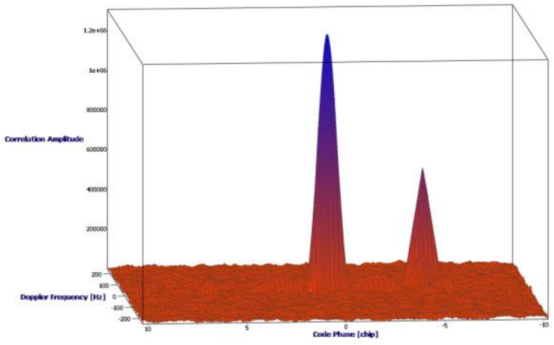


Figure 23: Multicorrelator-Plot of GPS PRN 6 when both peaks are separated by 5 chips from each other.

The reported trajectory can be seen in Figure 24, where on the right side the point cloud from the static phase and phase before the attack can be seen. The point cloud before the attack was smaller than in the static spoofing phase, thus static spoofing can also be interpreted as multipath spoofing.

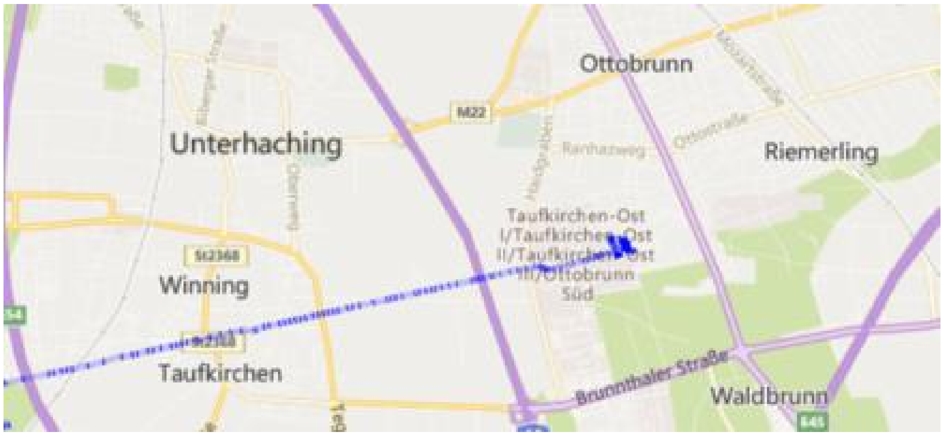


Figure 24: Trajectory of the spoofing attack from Ottobrunn, Germany (IABG), towards Taufkirchen

Figure 25, Figure 26, Figure 27, Figure 28 and Figure 29 show the SQM metrics DDM, DM, SRM, RM and the Moving Variance of DM. The correlator settings are described earlier in the theory part. The Moving Variance of DM is the variance of 15 DM values over 15 s, which describes the fluctuating behaviour of the correlation function asymmetry over time. PRN 7 is not shown here, because even if it showed a detection, the metrics were very noisy for this flat angle satellite and would therefore overwrite the other metrics. The DDM and DM show a clear increase in the standard deviation of the metric (fluctuations) for the time interval from the spoofing begin at 250 s till around 450 s. The SRM also showed this behaviour, but also a rise of the mean metric value, which stayed the same during the whole attack while the fluctuations decreased after around 450 s. The RM and Moving Variance of DM also showed an increase of the mean metric value during the whole attack, but the standard deviation of the metric slightly decreased. This illustrates that all those metrics can detect the attack via threshold exceeding and that this occurs for all satellites in a certain time window after the start of the attack. It can also be concluded, that all the epoch-based metrics (not Moving Variance metric) do not show a continuous detection over time due to the noisy behaviour. The Moving Variance and TFM have the ability to show a continuous detection over a certain time period. In general SQM can only show a detection till the correlation functions from authentic and spoofing signal are completely separated from each other, which depends on the velocity and acceleration of the spoofer. Metrics however can give false alarms also after the peaks are separated for example due to spoofer multipath and tracking inaccuracies. SQM metrics are generally sensitive to multipath, which can be seen for the flat elevated PRN 19 (purple), which shows visible deviations also before the attack. After the start of the accelerated position shift, the deviation of the metrics go down after around 430 s, depending on the satellite, which is the time window where the overlap of the correlation functions begin to vanish. Theoretically, the separation is faster for low elevated satellites due to geometric reasons, but since they also have more multipath in general, it is often difficult to separate these effects. All the metrics, especially the sensitive TFM can also show deviations after this point due to spoofer multipath or due to short tracking instabilities when changing an acceleration to a linear speed, which might be the case for PRN 17. Figure 30 shows the TFM for all the GPS L1 C/A satellites over time. The vertical black lines indicate the time window where all the satellites showed an alarm, which is per definition a spoofing alert in the receiver. The alert had a latency of around 20 s, meaning the spoofing attack could be detected in the receiver at 20 s after the beginning of the attack, but with a safety, that it is not multipath. This is the detection idea, looking at all satellites and excluding multipath, which occurs more randomly and not for all satellites at the same time, which is valid in open sky conditions and most likely also in not too shadowed areas. PRN7 and PRN 19 for example also show lots of multipath, which let the TFM rise at many moments in time before the attack. In the beginning (first 15 sec) the TFM often is 1, which comes from the PLL, which is not locked. After some seconds, when the PLL gets locked, the correlation function and therefore the TFM gets stable.

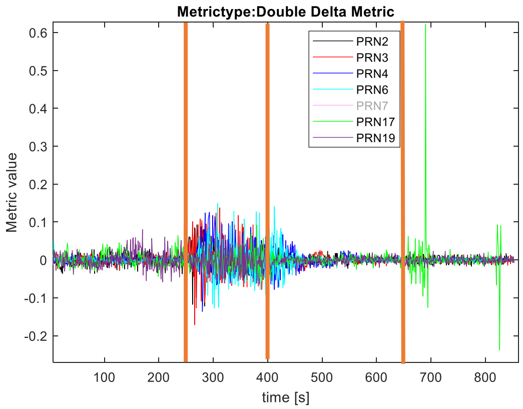


Figure 25: DDM for 6 satellites

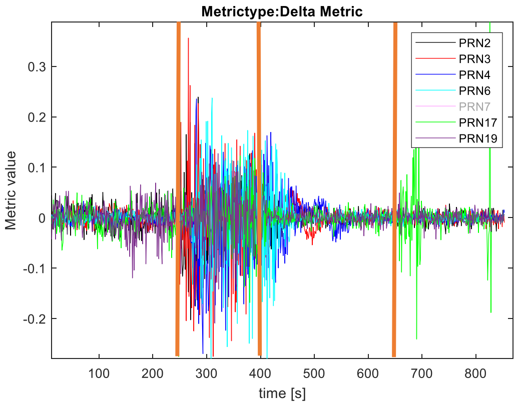


Figure 26: DM for 6 satellites

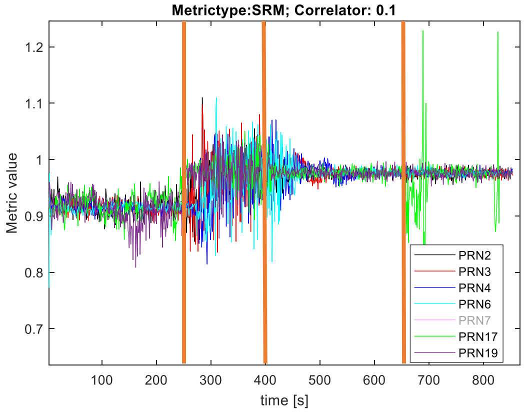


Figure 27: SRM for 6 satellites

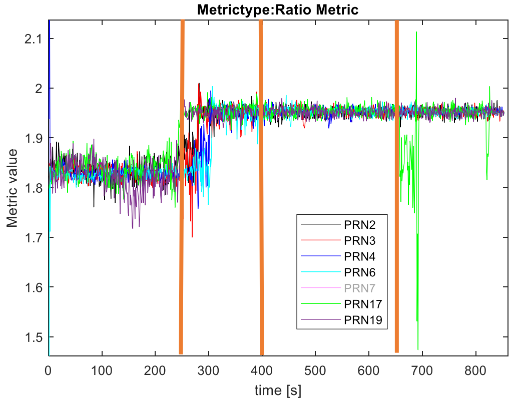


Figure 28: RM for 6 satellites

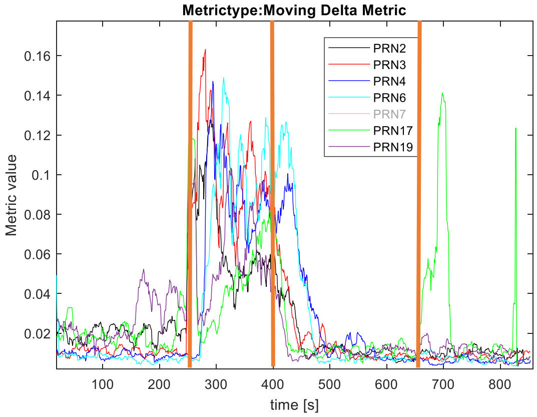


Figure 29: Moving Variance of DM for 6 satellites

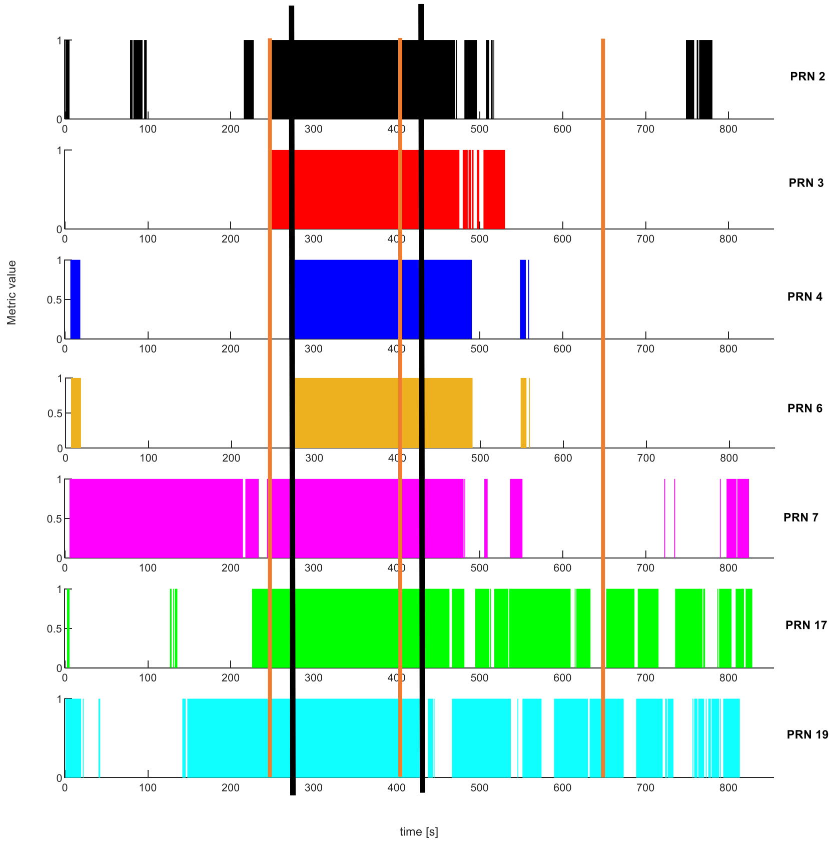


Figure 30: TFM for 7 different satellites over time. The two vertical black lines indicate the time interval, where all the TFM showed an alarm for all satellites, which is considered as spoofing alarm. The three orange vertical lines indicate (from left to right) the start of the spoofing, the start of the accelerated movement of the spoofer and the change from an accelerated to a linear speed.

All in all the investigated parameters showed a good detection ability and the results from the Septentrio with the SX3 were consistent, only the C/N_0 increase could not be seen for the Septentrio but the SX3, which remained unclear. There occurred so many small effects for all the parameters, that not all of them could be treated and described in this paper, but a follow-on paper is planned with more details.

IV. CONCLUSIONS

We performed a successful over the air spoofing attack and could trick three different COTS receiver. The position could be shifted smoothly kilometers away from the original coordinates. Several SQM metrics including the self-developed TFM metric and tracking parameters were investigated as spoofing detection parameters. Many parameters showed a significant deviation during the attack, meaning they could be used to successfully detect spoofing with the used spoofing settings. Several typical phases during an attack were analyzed, the stage before the attack, the static spoofing stage and the accelerated and linear position shift stage. With the help of a correlation function analysis, also the effects of the separation of the authentic and spoofing signal correlation peak could be shown. The fluctuation of the parameters and metrics decreased when the correlation peaks were separated. Since the attack was made for all receivers at the same time, the behavior of the three receivers could be compared. One unexpected result was that the Septentrio receiver could be spoofed successfully with only GPS L1 C/A and Galileo E1B/C spoofing signals, while the receiver was also using Beidou L1 and GLONASS L1 for the calculation of the PVT. The AGC of this receiver did not show a change during the attack. The receiver's position could be shifted kilometers away from the original position.

Funding:

The results presented in this work were developed within the project “Galileo Fusion”, funded by the German Federal Ministry for Economic Affairs and Energy (BMWi) and administered by the Project Management Agency for Aeronautics Research of the German Space Agency (DLR) in Bonn, Germany (grant no. 50NA2001).

Acknowledgement:

This research was supported by IABG Ottobrunn.

V. REFERENCES

[1] Montgomery, P., Humphreys, T., and Ledvina, B. (2009a). A multi-antenna defense: receiver-autonomous GPS spoofing detection. Inside GNSS, pages pp. 4(2):40-46.

[2] C4ADS (2019). Above us only stars, exposing GPS spoofing in Russia and Syria. https://static1.squarespace.com/static/566ef8b4d8af107232d5358a/t/5c99488beb39314c45e782da/1553549492554/Above+Us+Only+Stars.pdf.

[3] Ilie, I., Malo, S., Guilbault, R., and Kirk, T. (2017). Spoofing of electrical power grid: It's easier than you think. Proceedings of the 30th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+), Portland, Oregon, pp. 1383-1408.

[4] Yu, D., Ranganathan, A., Locher, T., Capkun, S., and Basin, D. (2014). Short paper: Detection of GPS spoofing attacks in power grids. WiSec '14: Proceedings of the ACM conference on security and privacy in wireless and mobile networks, Pages 99-104.

[5] Shepard, D., Humphreys, T., and Fansler, A. (2012). Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks. International Journal of Critical Infrastructure Protection, Volume 5, Issues 3{4, Pages 146-153.

[6] Akkaya, I., Lee, E., and Derler, P. (2013). Model-based evaluation of GPS spoofing attacks on power grid sensors. Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES), Berkeley, CA, pp. 1-6.

[7] R. Blum, D. Dötterböck and T. Pany, "Investigation of the Vulnerability of Mobile Networks Against Spoofing Attacks on their GNSS Timing-receiver and Developing a Meaconing Protection," Proceedings of the International Technical Meeting of The Institute of Navigation, pp. 345-362, 2019.

[8] Troglia Gamba, T., Truong, M., and Motella, B. (2017). Hypothesis testing methods to detect spoofing attacks: A test against the TEXBAT datasets. GPS solutions 21, pages pp. 577-589.

[9] Blum, R., Dütsch, N., Stöber, C., and Pany, T. (2020). New and existing signal quality monitoring metrics tested against simulations and time synchronized signal generator attacks. Proceedings of the 33th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS), pp. 2608-2618.

[10] R. Blum, D. Dötterböck, K. Han and T. Pany, "A new massive multi-correlator metric tested against GNSS signal generator attacks with a slow power increase and spoofer movement," Proceedings of the 2019 ISGNSS conference, 2019.

[11] Blanco-Delgado, N. and de Haag, M. U. (2011). Multipath analysis using code-minus-carrier for dynamic testing of GNSS receivers. Localization and GNSS (ICL-GNSS), 2011.

[12] Yuan, D., Li, H., Wang, F., and Lu, M. (2018). A GNSS acquisition method with the capability of spoofing detection and mitigation. Chinese Journal of Electronics, vol. 27, no.1, pages pp. 213-222.

[13] T. Pany, "Software Packages in Homepage of LRT 9.2, Universität der Bundeswehr Neubiberg, Germany," 2019. [Online]. Available: https://www.unibw.de/lrt9/lrt-9.2/software-packages/musnat.

[14] IGASPIN GmbH, Graz, Austria, "Homepage IGASPIN GmbH," 2020. [Online]. Available: http://www.igaspin.at/products.html.

[15] Stober, C., Kneissl, F., Eissfeller, Bernd, Pany, T., "Analysis and Verification of Synthetic Multicorrelators," Proceedings of the 24th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2011), Portland, OR, September 2011, pp. 2060-2069.

[16] Pini, M., Motella, B., and Troglia Gamba, M. (2013). Detection of correlation distortions through application of statistical methods. Proceedings of the ION GNSS + 2013. Institute of Navigation, Nashville, TN, September, pp 3279-3289.

[17] Troglia Gamba, M., Motella, B., and Pini, M. (2013). Statistical test applied to detect distortions of GNSS signals. International Conference on Localization and GNSS (ICL-GNSS), pp. 1-6.

[18] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O. Hanlon, and P. M. Kintner, “Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer,” in Proceedings of the 21st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2008), 2009, pp. 2314–2325.

[19] T. E. Humphreys, J. A. Bhatti, D. Shepard, and K. D. Wesson, “The Texas spoofing test battery: Toward a standard for evaluating GPS signal authentication techniques,” in Proceedings of the 25th International Technical Meeting of the Satellite Division of the Institute of Navigation 2012, ION GNSS 2012, 2012, pp. 3569–3583

[20] R. E. Phelts, “Multicorrelator Techniques for Robust Mitigation of Threats To GPS Signal Quality,” PhD Thesis, Stanford University, 2001