New and Existing Signal Quality Monitoring Metrics Tested Against Simulations and Time Synchronized Signal Generator Attacks

Ronny Blum[1], Nikolas Dütsch[1], Carsten Stoeber[2], Jürgen Dampf[1], Thomas Pany[1]

[1] Institute of Space Technology and Space Applications, Universität der Bundeswehr München, Germany
[2] Rohde & Schwarz GmbH & Co. KG, 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.

Carsten Stöber obtained his diploma in Geodesy from the Technical University Berlin. He worked in the field of GNSS as a research associate and R&D engineer at the Universität der Bundeswehr München, IFEN GmbH and Trimble. Currently he is working as a R&D engineer at Rohde & Schwarz in the GNSS signal simulator department.

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 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 the faculty of aerospace engineering where he teaches satellite navigation. His research includes all aspects of navigation ranging from deep space navigation over new algorithms and assembly code optimization. Currently he focuses on GNSS signal processing for Galileo second generation, GNSS receiver design and GNSS/INS/LiDAR/camera fusion. To support this activities, he is developing a modular GNSS test bed for advanced navigation research. Previously he worked for IFEN GmbH and IGASPIN GmbH and is the architect of the ipexSR and SX3 software receiver. He has around 200 publications including patents and one monography.

ABSTRACT

In this work we present the behavior of new and existing Signal Quality Monitoring (SQM) metrics under the influence of signal generator spoofing. Signal generator spoofing is the generation and emission of artificial authentic GNSS-signals, which tries to imitate the real satellite signals as good as possible to induce a wrong time and/or position output. The artificial signals must have a higher amplitude at the target position than the authentic signals to be tracked from the receiver. One at our institute investigated field of application, is GNSS based mobile networks, which are vulnerable to spoofing [1].

SQM metrics generally investigate the shape change of the correlation function (CF), which can occur due to multipath, spoofing or satellite payload hardware errors. We investigated synchronized attacks with the purchasable LOKI- Jamming and Spoofing generator from IGASPIN GmbH [2] and with MATLAB based simulations. Synchronized means that the spoofing signal synchronizes the code phase, the Doppler and the navigation data to the real satellite signal, fitting the incoming authentic signal at the target receiver location. The location of the target has to be estimated as good as possible to get the best results. Since synchronized attacks nowadays cannot be detected or mitigated by typical COTS (commercial of the shelf) receivers and many but not all receivers also acquire and track unsynchronized spoofing signals, spoofing protection in the receiver is needed. One way is to look for anti-spoofing-parameters in the receiver, including SQM-methods. The LOKI-Spoofer 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.

We implemented a new metric for spoofing detection for Galileo E1B and GPS L1 C/A signals in our software receiver MuSNAT [3], which we call Threshold Fluctuation Metric (TFM). It is a slight modification of the fluctuation metric in [4]. We compared the results of the proposed metric with the results for the well-known metrics Single Sided Ratio metric, the Double-Delta metric and the Delta metric and tested the metrics against the signal generator attacks and MATLAB based simulated spoofing attacks. Furthermore, the paper presents also a fully synchronized position spoofing attack with three well known receiver.

For the simulations the TFM showed better results when the C/N_0 was changing significantly. In this case the Double-Delta, the Single Sided Ratio and the Delta metric gave false alarms. Also during the spoofing attack, the new metric showed a more continuous detection rate and can therefore be considered as more reliable and stable. For a certain speed range with low speeds and a not too high spoofer gain the TFM could also detect the movement of the spoofer without a start delay to the target. We therefore recommend to use the TFM instead of the other investigated metrics.

The LOKI spoofer experiments were made over cable. Since the delay can only be set in 100 ns steps, we could not test a perfect alignment of the code phase from the spoofer signal to the authentic signal. The smallest achievable code delay was about 15 m, where the TFM and the Single Sided Ratio metric could detect the attack in contrary to the Delta and Double-Delta metric. The position could be successfully shifted away for all investigated receivers (Septentrio PolaRx5TR, U-Blox M8T and IFEN SX3). Even with RAIM (Receiver Autonomous Integrity Monitoring) mode on, the Septentrio PolaRx5TR receiver could be spoofed. The anti-spoofing flag of the U-Blox M8T did not detect the spoofing attack.

In order to distinguish a spoofing attack from normal multipath for the TFM we analyzed the results of many satellites, since multipath in contrast to spoofing transmission from one spot generally does not affect all satellites in the same way. This paper also shows how multipath affects the TFM on real signals captured with a roof antenna. The TFM can also be used for multipath detection. At the beginning of the LOKI spoofing attack, the TFM of all satellites were affected at the same time, which lead to a spoofing alert in our receiver.

Keywords: GNSS, SQM, metrics, spoofing, anti-spoofing, signal generator attack

I. INTRODUCTION

GNSS signals are vulnerable to spoofing and jamming due to the low signal power. Spoofing is the intended manipulation of the position and time result of a GNSS receiver. A recent successful spoofing of ships could be achieved in [5]. Different types of spoofing attacks exist, ranging from simple to highly sophisticated.

The simplest is the record and replay attack, where a signal is recorded with a software radio and later emitted with the same device. There are still lots of receivers which have no methods implemented to defend such simple attacks [1]. Another simple approach is the unsynchronized signal generator attack. It uses artificially generated signals, which try to imitate the real signal, but which typically do not transmit an authentically predicted navigation message or which do not achieve code synchronization.

More sophisticated is the meaconing attack, where the GNSS signal is captured with an antenna, amplified and retransmitted with another antenna. This induces a small delay and therefore a change in the position and time. Also encrypted signals can be spoofed with this sort of attack, because the encryption code does not need to be known when just performing a re-transmission.

More sophisticated are time synchronized signal generator attacks, which also shall be investigated in this paper. The artificially generated signals are generated in the way, that the target receiver gets the spoofing signal with the same navigation message, synchronized code phase and in the best case the same Doppler than the authentic signals. If the navigation message is predicted, the spoofer has to get the navigation message from the GNSS signals directly (as in our case), or from the internet. The only disadvantage is, that all spoofing signals come from one spot, which can be potentially detected with a multi-antenna array [6], [7], or with a spatially moved antenna and known trajectory [35]. Both methods are however expensive and complex in terms of setup.

The most sophisticated attack uses more than one emitter, one emitter per fake satellite. Therefore the spoofing signal does not come from one spot.

The clock error spoofing is a more unknown approach, which only tries to irritate the time of the target receiver. This was investigated and successfully performed at our institute to manipulate the 10 MHz output of a GNSS timing receiver.

The spoofing detection is a wide field, several approaches have been done in the past. Beside a multi-antenna array and encrypted signals, there is the possibility of using additional sensors like gyroscopes or acceleration sensors. A table of spoofing methods and countermeasures are given in [1]. Countermeasures with general receiver software methods are shown in [8], [9], [10], [11], [12], [13] and [14]. For example, a software approach using anomalies in the C/N$_0$ is proposed in [15] or, using the acquisition stage against spoofing in [16]. The influence on the receiver tracking loops during a spoofing attack is investigated in [17] and a characterization of the receiver response to spoofing is given in [18].

Originally, Signal Quality Monitoring (SQM) methods, which investigate correlator function values, were proposed to detect multipath ([19], [20] and [21]) or satellite hardware failures (so called Evil Waveforms) [22]. In the last years SQM methods were more and more investigated and proposed as anti-spoofing methods, since also in this case the shape of the correlation function changes due to the overlay of the spoofing signal to the authentic signal. SQM papers against spoofing can be found in [23], [24], [25], [26], [27], [28], [29] and [30]. In [31] the performance of SQM metrics against spoofing is investigated and in [32] the Single Sided Ratio metric is considered against spoofing, which is also investigated in this paper beside other metrics. Distinguishing multipath from spoofing is also important for a working anti-spoofing software, this was for example investigated in [19] and [20]. A paper about spoofing in general can be found in [33].

A SQM-metric is in general a mathematical operation on correlation values, which should give a different result when multipath, spoofing or Evil Waveforms occur. We implemented the Single Sided Ratio metric, the Double-Delta metric, the Delta metric and a new metric, which we call TFM, in our own software receiver MuSNAT [3]. In this paper we compared those 4 metrics in terms of detection rate and false alarm rate. To generate spoofing signals we used the simulation tool YASST (Yet Another Signal Simulation Tool) and the purchasable LOKI-Spoofer from IGASPIN GmbH [2]. YASST was developed at our institute and is a MATLAB/CUDA based GNSS signal simulation tool. In this work we developed a spoofing module for YASST, which can generate single satellite signals for authentic and spoofing signals for GPS L1 C/A and Galileo E1 B/C. With YASST we investigated unsynchronized signal generator attacks and further details are summarized in Chapter II.5. With the LOKI-Spoofer we investigated time-synchronized signal generator attacks with over the cable transmission. Over the air transmission is also planned for the future.

In [4] we developed the fluctuation metric, which is the standard deviation of the multicorrelator values over a time period of 15 s (so called moving standard deviation), each correlator value normalized with the prompt correlator value. The values were compared with theory values, which represent the theoretical noise-only-results of the metric values without the influence of multipath or spoofing. The higher the difference between theoretical noise only and measured metric values, the more the influence of multipath or spoofing. This time we did not implement the theory comparison, but simply the noise only thresholds, which we determined with YASST simulations.

Reference [23] also investigates fluctuations of the CF for spoofing detection with a moving variance, but without comparing to theoretical values or simulated noise only values. In this paper we show, that the use of the moving variance or standard deviation without comparison to noise-only simulated values or noise-only theoretical values leads to frequent false alarms, when the C/N$_0$ changes significantly and abrupt. The C/N$_0$ can change due to signal blockage, for example when the signal path gets interrupted by a tree, or due to multipath itself. Also unintentional interference or intentional jamming could deteriorate the C/N$_0$ values. Therefore, we show that our metric with the comparison to the noise only values is a big improvement in terms of the false alarm rate. In terms of metrics, which only takes a single metric value and not values over a time period like the standard deviation, we show, that these metrics are in general too noisy, which comes from the noise itself but also due to the often changing relative phase of the spoofing signal to the authentic signal in the signal overlap time. This phase change occurs due to the different Doppler values, which is generally the case for this sort of spoofing attack. Single metric values are for example the Delta, the Double-Delta and the Single Sided Ratio metric, which we further explain in II.2. The authors in [23] also came to the conclusion that single metric values are not very effective to detect spoofing because of the noisy behavior. If the values are smoothed, the noise disappears, but then the spoofing signal would also be smoothed, which can lead to high misdetection rates.

To distinguish multipath from spoofing, we compare the results of all tracked GPS L1 C/A and Galileo E1B/C signals. It is unlikely, that multipath occurs at the same time for all satellites due to the different angles of the line of sight of user to satellite. In general only a few satellites show multipath at the same time, but a spoofer, which sends his signal from one spot with one antenna, changes the correlation signal for all satellites at the same time. This is exploited in the software. Satellite payload errors in many satellites at the same time is also unlikely, even for one satellite it is unlikely. Therefore this can also be excluded by considering many satellites.

One other advantage of our proposed metric is the multicorrelator usage. In the past, only a few correlators were used, but we implemented the fluctuation metric with the use of 37 correlator values in the whole correlation function area. This means, that also fluctuations at the edge of the correlation function will be considered, which leads to a higher detection probability of spoofing with higher start delays between the spoofer and the target receiver. The software could also be upgraded for other GNSS signals.

II. THEORY, METHODS AND MEASUREMENTS

II.1 Signal model and window of overlap

A spoofing attack can be generally explained in the correlation process in the receiver. When the spoofer signal has a higher signal amplitude than the authentic signal, the receiver switches to the correlation peak of the spoofer. In the transition time between the lock of the authentic and the lock of the spoofing signal, the correlation function gets distorted and fluctuations occur (Figure 1). But also when the spoofing signal is tracked, fluctuations occur due to a different Doppler or code phase offset from spoofing and authentic signal. This is also the case for a high sophisticated spoofer, when he tries to shift the position and time away from the authentic position and time. Then the spoofer uses a certain Doppler to achieve that. Therefore we think, that fluctuations occur in the most cases, even for the highest sophistication of spoofing, because the position/time always have to be shifted away. 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. But high gains we saw often lead to tracking interruption, which is also noticeable for a static open sky antenna. In [3] we showed, that the fluctuation metric detects the shifting attempt of the spoofer. During the shifting process, the correlation peaks from authentic and spoofing signal move apart more and more till the overlapping process stops when both correlation functions are completely separated. After this point, none of the investigated metrics can detect the attack, because the fluctuations only occur due to the overlap. This time window of overlap is in general used in the SQM-metrics. The time window depends on how fast the spoofer shifts the correlation function. We found out that a very slow shifting (<0.01 m/s) is in general harder to detect, because the fluctuations due to the Doppler difference lead to less fluctuations in this case.

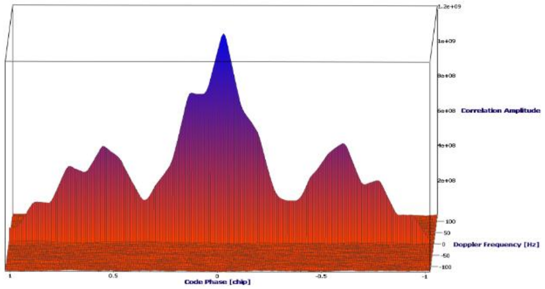

Figure 1: Correlation function of a Galileo E1B signal during the beginning of a spoofing attack, taken with IFEN SX3 software receiver

To express the spoofing process in the overlap window in formulas, we first declare the whole CF R(τ) in (1 (τ is the code phase), which is the addition of the authentic CF R$_a$(τ) and the spoofer CF R$_s$(t, τ), which is time dependent, because the spoofer will try to shift the peak after the successful tracking of the spoofing signal. The noise $n(t, \tau)$ is also time dependent, since the CF of the authentic signal contributes to the noise floor itself after the tracking of the spoofing signal and the spoofer generally also have a different C/N$_0$. Therefore the C/N$_0$ normally changes after the start of the attack.

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

The CF of the spoofer is given in (2:

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

$\tau - \tau_s(t)$ is the time dependent code phase difference from the spoofer to the authentic signal. For 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. φ_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 amplitude of the spoofer, which is time dependent, when for example the power is increased slowly. This we have investigated in [3] and is more difficult to detect, because parameters like the C/N$_0$ and the power don't show jumps anymore. Also in some cases the parameter code minus carrier (CMC) does not show a jump behavior.

II.2 Single Sided Ratio Metric, Delta Metric and Double-Delta Metric

In this subchapter we introduce the 3 older well-known metrics, the Single Sided Ratio Metric, the Delta Metric and the Double-Delta Metric, which we used with our multicorrelator setup. They are most often used in the literature, for example [21], [34] and [32] investigated the Single Sided Ratio Metric. This metric (also known as asymmetric ratio or just ratio test) is usually defined as the late correlator value divided by the prompt correlator value, (3 represents the metric, x is the code phase, which is different for every correlator. In our case, since we used 37 correlators, we tried all kind of multi correlator values for *x*, but in the literature normally only the late correlator (for example often 0.2 chip, narrow correlator) was used. The reason for considering this ratio metric is that the late side of the correlation curve is usually more distorted by multipath or spoofing.

Single Sided Ratio Metric:

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

The Delta Metric is given in (4 and is also called symmetric ratio test. In the literature *x* and –*x* are most often the late and early correlators, we investigated all kind of multicorrelator values for *x*. 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 noise, multipath itself or ionospheric scintillations. Without the normalization the metrics would be falsified and no useful results would be possible.

Delta Metric:

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

The Double-Delta metric is defined in the literature as the difference between 2 late-early correlator pairs, normalized by the prompt correlator. We also used here all our multicorrelator values for *x* and *y* but always with the condition *x* > *y*
Double-Delta Metric:

$$DD = \frac{(C_{-x} - C_{+x}) - (C_{-y} - C_{+y})}{C_0} \qquad conditions\colon\ x > y \tag{5}$$

The authors in [13] and [18] investigated the nominal statistics of the aforementioned metrics for BPSK(1) and BOC(1,1) signals [Table 1] . BPSK means Binary Phase Shift Keying, BOC Binary Offset Carrier. In Table 1 the correlators with 0.5 chip width and 0.1 chip width were used. The variance is dependent of the inverse of the integration time T and the C/N$_0$ for both modulations. BPSK(1) is used for GPS L1 C/A signals and BOC(1,1) can be used as an approximation for the CBOC signal, used in the Galileo E1B signals. This illustrates the aforementioned drawback of these metrics, the dependence on the C/N$_0$, which can change during measurements.

Table 1: Nominal mean and variance for specific early late correlator values for the in the paper used metrics Single Sided Ratio, Delta and Double-Delta [13], [18]

SQM metric	*Definition*	*Nominal mean BPSK*	*Nominal variance BPSK*	*Nominal mean BOC(1,1)*	*Nominal variance BOC(1,1)*

Single Sided Ratio	$\frac{C_{+0.5}}{C_0}$	0.5	$\frac{0.75}{2TC/N_0}$	-0.5	$\frac{0.75}{2TC/N_0}$
Delta	$\frac{C_{-0.5} - C_{+0.5}}{C_0}$	0	$\frac{2}{2TC/N_0}$	0	$\frac{2}{2TC/N_0}$
Double-Delta	$\frac{(C_{-0.5} - C_{+0.5}) - (C_{-0.1} - C_{+0.1})}{C_0}$	0	$\frac{1.6}{2TC/N_0}$	0	$\frac{2.4}{2TC/N_0}$

In order to cancel out the C/N$_0$ dependence we developed the fluctuation metric, which we describe in the next subchapter.

II.3 Threshold Fluctuation Metric TFM

The Threshold Fluctuation Metric TFM at a specific time is the mean over all 37 standard deviation values of the with the prompt correlator value normalized correlator values over a batch of 15 seconds. The number 37 comes from the amount of correlators which were used here. The metric therefore describes the fluctuations from all 37 correlators. The correlators were spread over the whole chip distance with equal spacing (Table 2). In general it is possible to increase the number of correlator values up to 201 in our software receiver, but then the sampling rate has to be changed from 20 to 100 MHz. At this point we have not investigated, if the results in terms of spoofing detection get better with 201 correlators. This might be a future task. It is also unclear, if the calculation time will be much worse in this case.

Table 2: Correlator positions, given in distance to prompt correlator in [chip]. In total 37 correlators were used.

0.0	+/- 0.05115	+/- 0.10230	+/- 0.15345	+/- 0.20460	+/- 0.25575	+/- 0.30690	+/- 0.35804	+/- 0.40920	+/- 0.46034
+/- 0.51149	+/- 0.56264	+/- 0.61379	+/- 0.66494	+/- 0.71609	+/- 0.76724	+/- 0.81838	+/- 0.86953	+/- 0.92068	

The integration time can be set in our software receiver, we choose 64 ms for GPS L1 C/A and 132 ms for Galileo E1B (no specific reason). This time span is used every second to generate correlation values, therefore for GPS L1 C/A around 935 ms and for Galileo E1B around 869 ms are not used in a 1 second time interval. This was implemented to fit our RINEX format, but could be theoretically changed to a continuous value output.

The metric TFM for a specific time t is given by:

$$TFM_t = MS - NT = \frac{\sum_{x=1}^{37} std\ RM_{x,t}}{37} \text{ - NT} \qquad (6)$$

$NT\ = Noise\ only\ threshold, determined\ by\ YASST\ simulations$
$MS\ = Mean\ of\ standard\ deviations\ over\ the\ correlators$

x is the correlator position. The sum is built over all standard deviations of ratio metrics *RM* from each correlator position and then it is divided by the amount of correlators 37 to get the mean standard deviation of the *RM*'s over all correlators. This value is compared with the noise only threshold, built by our MATLAB based simulation tool YASST. YASST therefore generates GPS L1 C/A and Galileo E1B/C signals (CBOC, Composite Binary Offset Carrier) without multipath (noise only), which are read in and processed by the MuSNAT, which gives out the noise only influenced values of *MS* to cancel out any C/N$_0$ based effects in the metric. The threshold is built for each C/N$_0$ value from 35 to 55 dBHz in 3 dB steps, where the threshold is the value which is not exceeded in a one hour signal duration plus a slight self-chosen buffer of 0.05. Since only signals with a C/N$_0$ in 3 dB steps are made, an interpolation of the results is made in the end to get the threshold for each C/N$_0$ value in a mathematical fit equation (Figure 2). The values from the equations in Figure 2 were taken for the noise only threshold values *NT*. The used signal bandwidth of the YASST signal was 20 MHz and the IF was 2.5 MHz.

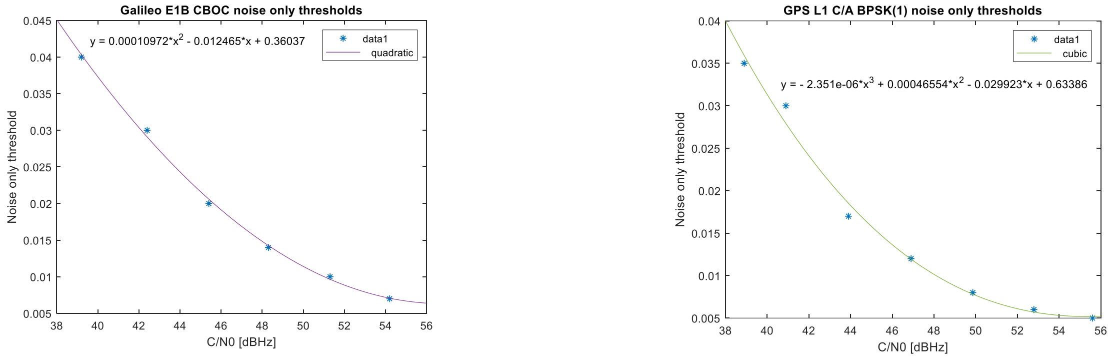

Figure 2: On the left the fit curve and fit equation for the noise only threshold (NT) in dependence of the C/N$_0$ for the Galileo E1B CBOC YASST simulated signals. On the right for the GPS L1 C/A YASST simulated signals.

The standard deviation for a single correlator position *x* is given by (7, where the time interval from *t*-15 seconds to *t* is taken, also called one batch *b*:

$$std\ RM_{x,t} = \sqrt{\frac{\left(\sum_{b=t-15}^{t}(\frac{C_{x,b}}{C_{0,b}} - Mx)^2\right)}{14}} = \sqrt{\frac{\left(\sum_{b=t-15}^{t}(\frac{C_{x,b}}{C_{0,b}} - \left(\frac{\sum_{b=t-15}^{t}\frac{C_{x,b}}{C_{0,b}}}{15}\right))^2\right)}{14}} \tag{7}$$

Mx is here the mean over the considered 15 s time period of the prompt correlator normalized correlator value x:

$$Mx = \frac{\sum_{b=t-15}^{t}\frac{C_{x,b}}{C_{0,b}}}{15} \tag{8}$$

Note that the standard deviation is defined as the square root of the mean quadratic deviations of the mean.
In each measurement batch of 15 seconds, the average C/N$_0$ from this measurement time span is taken and the noise only threshold for this C/N$_0$ value is taken to compare the measurement *MS* with the noise only threshold *NT*.
If the TFM is then >0, a so called multipath/spoofing flag goes on for this satellite and TFM is set to 1. All satellites were compared and if TFM is changing to 1 for all satellites at the same time, a spoofing alert is written out. The metric is recommended to use only in open sky conditions and not under heavy multipath influence like in the forest. In a rural area between houses, we think the metrics can still be used, if at least a partly open sky condition is present.

II.4 The signal generator LOKI-Spoofer and the measurement setup

With the LOKI spoofer (Figure 3 right) position and time spoofing attacks can be performed. It has the ability to spoof in real time, which means, that the faked signal can be aligned in code phase, Doppler and navigation message content to the genuine signal. In an interactive mode new spoofed positions can be added to the spoofed trajectory even if the spoofing scenario already runs. In Figure 3 a brief overview of the LOKI spoofer components are given. The internal IFEN SX3 GNSS receiver tracks the Live-GNSS signal and steers the USRP which in turn delivers a stable carrier frequency. The SX3 performs also the code phase and Doppler measurements which are needed for the generation of the spoofing signal. The navigation message of the spoofing signal is built by extracting the navigation message content of the real signal. The spoofing signal is generated via software in the notebook by estimating the code phase and Doppler at the target position. Therefore the target coordinates have to be known and they have to be set in the LOKI spoofer in advance. An external notebook controls the SX3 and the USRP. By using the notebook, different spoofing trajectories can be defined and loaded into the LOKI. This can be done either in advance of the attack by defining different waypoints in a chronological manner or interactively during spoofing. The USRP up-converts the spoofing signal to the L1 frequency which then can be transmitted to the target receiver by using a directional spoofing antenna. For over the air spoofing tests it is important to have a good isolation between the transmitted spoofing signal and the received genuine signal to avoid the feedback of the spoofing signal into the reception path.

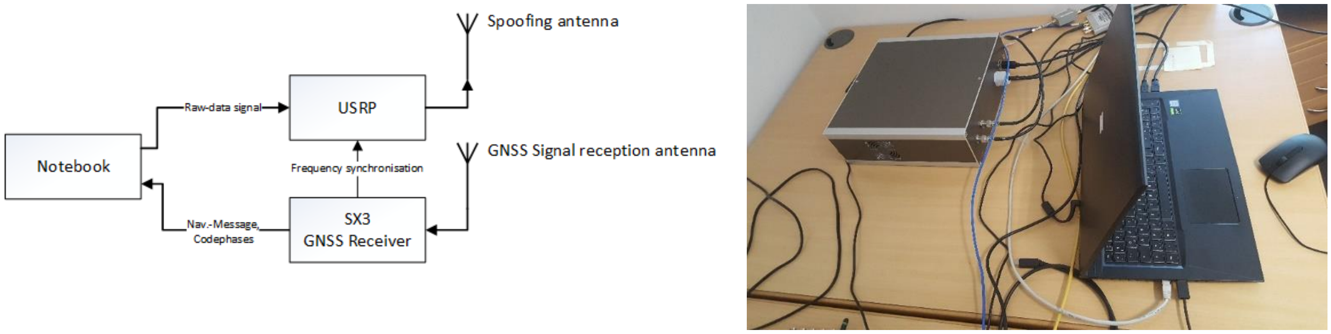

Figure 3: Left: Internal structure of the LOKI spoofer, right: LOKI spoofer (box) with notebook

The LOKI-Spoofer 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 4 we see the measurement setup for the LOKI spoofer experiment. A second frontend (IFEN SX3) was installed to track the spoofing signal only. There is also a jammer installed in the LOKI spoofer, which we did not use in this work.

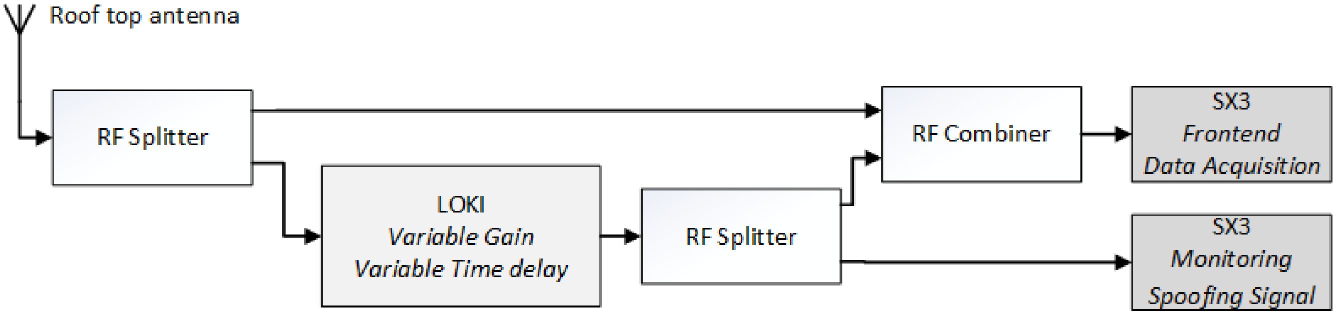

Figure 4: Measurement setup of the LOKI spoofer over the cable experiment. In order that the spoofing signal is higher than the authentic signal, gain and additional attenuators can be changed.

The spoofing signal and the real signal were fed to the target receiver by using a Radio Frequency (RF) combiner. The genuine signal from the institute's roof top antenna was split to have a reference signal for LOKI's internal SX3 receiver. 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 genuine signal would not affect the receiver's tracking loops. A 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.

II.5 The simulation tool YASST

YASST (Yet Another Signal Simulation Tool) is a MATLAB/CUDA based signal simulation tool. Till now one PRN (Pseudo Random Noise) can be simulated for Galileo E1B/C, PRS-Like and GPS L1 C/A and L2. Also potential E1D signals can be generated, a BPSK signal with offset to the L1 frequency. First two baseband signal snapshot are generated in MATLAB, one for each navigation data symbol 1 and -1. All signals, which shall be generated are then summed up. Then the CUDA-program takes the two snapshots and up converts the baseband signal on the carrier (for example L1: 1,575 GHz) and considers the navigation message, which is a text file that has to be read in the code. Basically, it combines the snapshots to the full signal according to the navigation message information. User dynamic can be added in form of a changing Doppler, the information has to be set in the initialization file. The program can generate several file formats: 2, 8 and 16 bit with an intermediate frequency. Also another special file format with a repeating I, Q-value combination can be generated, which is needed for using a USRP (Universal Software Radio Peripheral) from National Instruments to transmit signals over the air. YASST can generate signals with a certain C/N_0 value, frequency-filter to simulate front-ends, secondary code, navigation message or ionospheric delay. The source code is made in that way, that also other BOC and BPSK signals can be generated with a special initialization file.

There are two modules included, one for performance analysis and the other for spoofing simulation. In the performance analysis module waveform, spectrum, cross correlation function, multipath envelope, PLL, DLL and FLL noise can be simulated and plotted. Figure 5 shows the used Galileo CBOC waveform, the spectrum of the baseband signal, which was generated for the used Galileo E1B signal, a snapshot of the real and absolute CBOC-signal and the PRN code (blue curve).

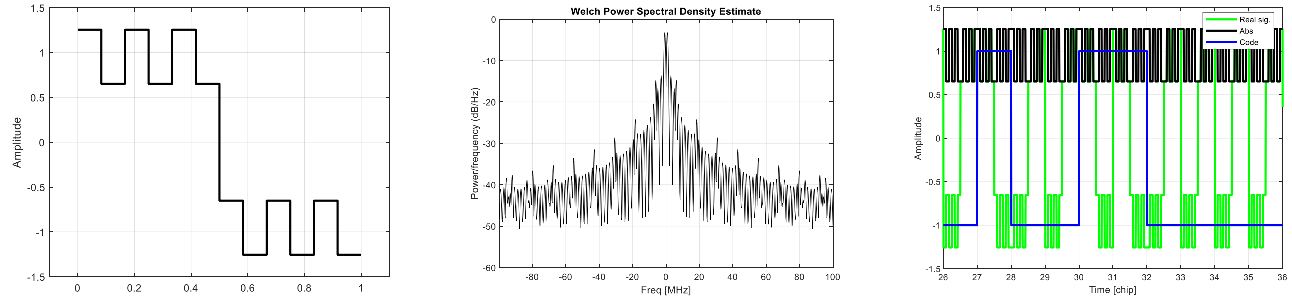

Figure 5: Left: For the YASST spoofing simulation used Galileo E1B CBOC chip shape. Middle: Spectrum of the E1B CBOC baseband signal (note the CUDA program later samples this signal with a lower sampling rate of 20 MHz) Right: Signal snapshot of the Galileo E1B CBOC signal with PRN code in blue.

The spoofing module can generate a simulated authentic and a spoofing signal. Also the overlap from both signals to one signal can be done. The approach with the two signals can be used for the transmission of a dual-in-and-output USRP for over the air experiments. The USRP reads then both signals in and transmits both from two different antennas. The approach with one signal, the overlap signal, is used in this paper. This signal can be read in and processed by the MuSNAT receiver directly and the spoofing influence can be analyzed. The metric values obtained within the signal processing are written out in a text file. Several parameters can be set in the spoofing module:

- Turning spoofing module on and off
- Start time of spoofing attack
- File duration
- Start delay of spoofer
- Speed of spoofer and authentic signal
- C/N_0 of authentic and spoofing signal each
- Gain of the spoofer compared to the authentic signal
- Turning off and on a slowly increase of the power, called ramp
- Time till the ramp reaches final gain value, called ramp duration

III. RESULTS

III.1 Simulation results

In this result chapter we show the simulation results with the YASST simulation tool. First, a drop of the C/N_0 for a Galileo E1B CBOC signal was made to illustrate the behavior of the different metrics. The drop simulation is shown in Figure 6. The C/N_0 drops 8 dB at around 120 s. We see the problem of the high noisy behavior of the Single Sided Ratio-, the Delta- and the Double-Delta metric. Also after the C/N_0 drop, the noise increases significantly with a clear higher probability of false alarms due to the occurring higher values. We can see later, that also spoofing can provoke metric rises, which let the metrics reach similar values than in this C/N_0 drop series. Therefore we do not recommend these metrics against spoofing, but they could be improved by implementing a C/N_0 dependent threshold. The MS-metric (Figure 6, lower plot) also increases, which is as expected. The TFM-metric, which cancels out C/N_0 effects, shows always 0, which means, that no alarm is given. An alarm would be the value 1. This demonstrates one of the advantages of the TFM-metric compared to the other investigated metrics. Note that in all the plots in this chapter it took around 15 seconds to get a PLL lock in the beginning, therefore the metrics partly show outliers in this time span. The TFM was implemented, that it only starts after PLL lock.

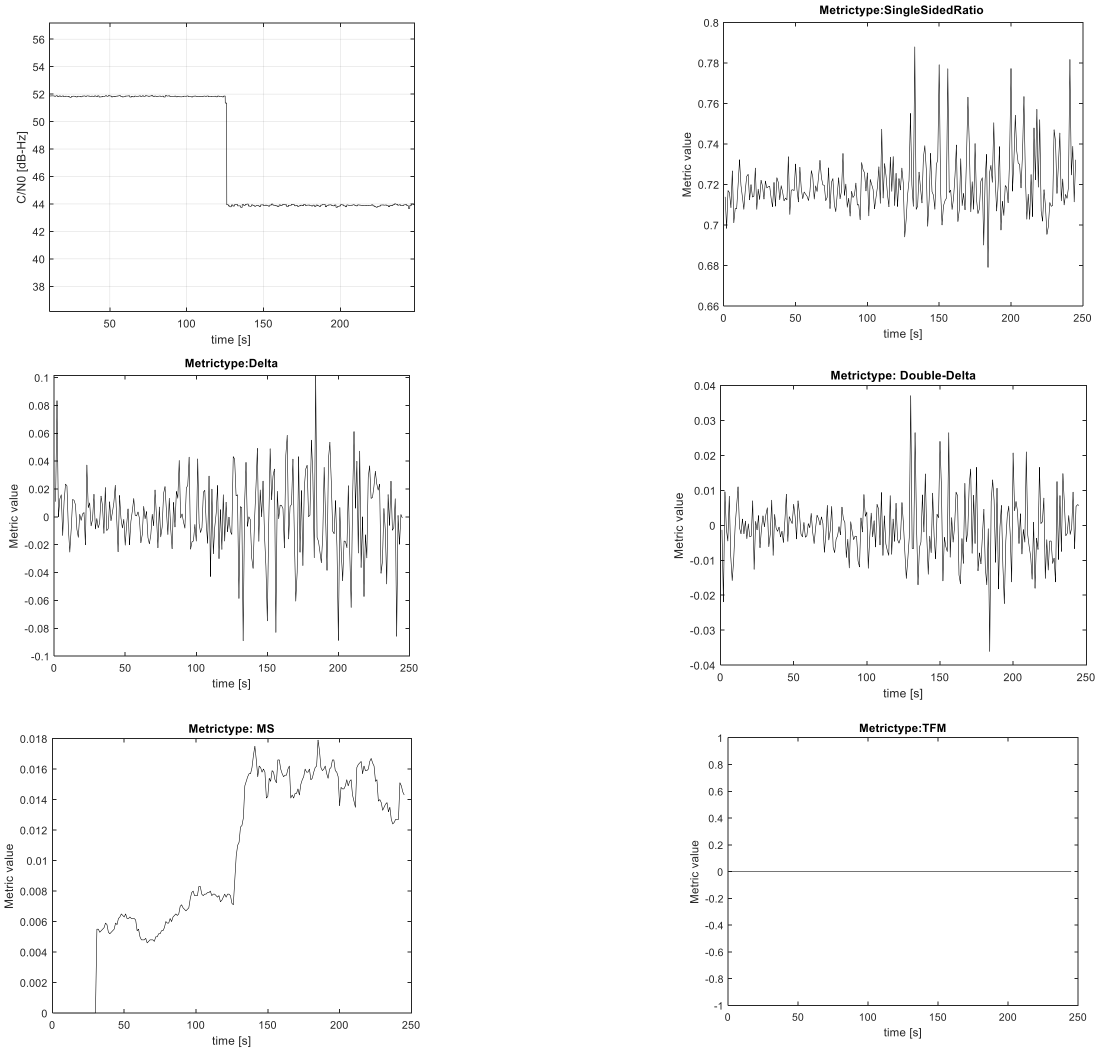

Figure 6: Left upper: C/N$_0$ over time, the fall at around 120 s can be seen. Right upper: Single Sided Ratio metric with correlator offset 0.01023 chip ((3). Left middle: Delta-Metric with correlator offsets 0.01023 chip and -0.01023 chip ((4). Middle right: Double-Delta metric with correlator offsets 0.05115 chip, -0.05115 chip, 0.01023 chip, and -0.01023 chip ((5). Left lower: MS metric ((6). Right lower: TFM-Metric ((6).

Similar results were got with a sudden increase of the C/N$_0$ and also for C/N$_0$ oscillations with different oscillation frequencies, also for the GPS L1 C/A signal. The TFM always showed no alert, where else the other metrics had a noisy behaviour with single big increases of the metric values, also for several other taken correlator values in the whole chip area.

In Figure 7 the YASST spoofing simulation results are presented for a spoofer start delay of 30 m. This means that the code phase distance at the beginning of the attack between spoofer and target is 30 m. No spoofer speed is set here. Till 125 s only the authentic Galileo E1B CBOC signal with a C/N$_0$ of 41 dBHz is present. At 125 s the spoofing signal with a C/N$_0$ of around 47 dBHz is added with a gain of 5 dB. Note that the C/N$_0$ change is only about 1 dB and not 5 dB, which we think is because of fading and the fact, that the authentic signal remains as additional noise when the spoofing signal is tracked. The sudden code phase jump induced from the tracking switch from the authentic to the spoofing signal let all the metrics rise at 125 s. However the TFM shows a longer alert (metric value=1) where else the other metrics only show a very short time metric rise followed by a sudden decrease. Due to fading effects from the spoofing with the authentic signal, the C/N$_0$ of the spoofer was only around 1 dB stronger, which is due to the relatively low gain of 5 dB.

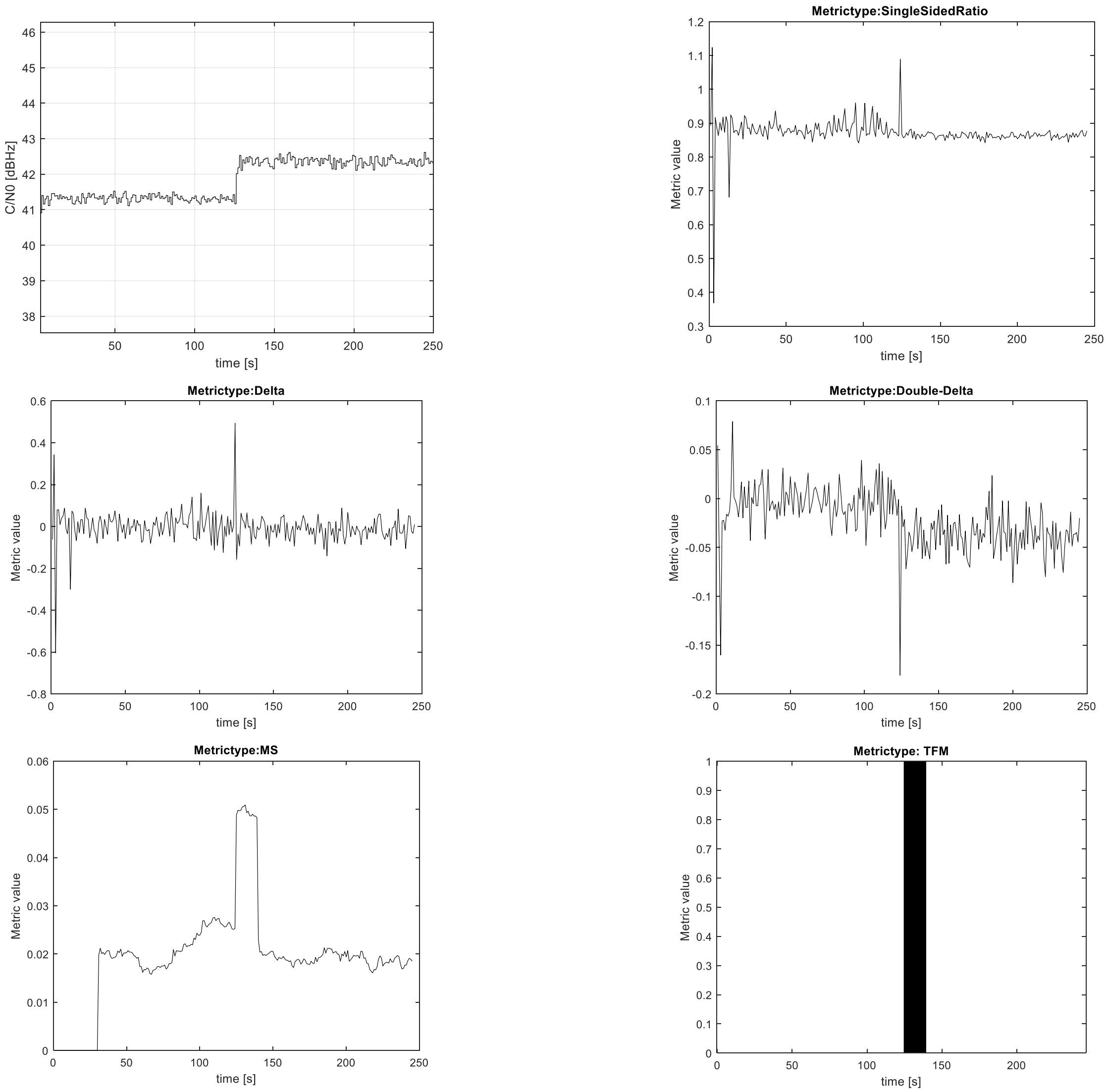

Figure 7: C/N_0, Single Sided Ratio-, Delta-, Double-Delta-, MS- and TFM in a YASST spoofing simulation. The Single-Sided ratio metric used the correlator at the chip position 0.1023 chip, the Delta metric used the correlators at +/- 0.1023 chip ((4), the Double-Delta metric at +/- 0.1023 chip and +/-0.05115 chip ((5). After 125 s the spoofing starts with a delay of 30 m. The spoofer used a gain of 5 dB and a C/N_0 of 47 dBHz, which was not reached at the attack due to fading effects from the spoofing signal with the authentic signal, only around 42.5 dBHz. All metrics detected the attack in this case.

In Figure 7 a start delay of 30 m was used, which led to massive fluctuations. Start delays of 0 m are very difficult to detect, but also very difficult to achieve for the spoofer, since he has to estimate the target position perfectly to match the code and carrier phase. When the spoofer increases the distance after the take-over of the control of the target receiver, the spoofer must use a different Doppler to achieve that. If the Doppler is too high, a jump in the Doppler occurs and could be detected via simple Doppler observation, however a small acceleration can be used to avoid jumps. For low Doppler values, the overlap of the spoofing signal with the authentic signal leads to fluctuations of the correlation function due to fading. The TFM can detect this behaviour (Figure 8) quite well, the other investigated metrics not. The attack started at 180 s. It took around 40 s, then the TFM showed a continuous detection at around 220 s till around 450 s, then the continuity went down. We think, that the reason for the 40 s till the TFM rose is that the correlation functions were aligned too much in the beginning and therefore no significant fading effects occurred. When time progresses, the correlation functions moved apart and after 40 s the fading effects seemed to let the metric rise. At around 480 s the detection went completely off, which is because then no overlap of spoofing and authentic CF is present anymore. We found out however, that the TFM can only detect speeds from around 0.01 till 2 m/s. This also means when the spoofer uses an accelerated movement instead of a constant speed, these low speeds from 0.01 to 2 m/s always occur in the beginning of the acceleration phase. Therefore, accelerated spoofer movements should be detectable.

However we did not investigate this aspect in this work. So the TFM has a good potential to detect a spoofer with a start delay of 0 m, if a spoofer movement follows (which normally happens). All in all, compared to the Single Sided Ratio, Delta and Double-Delta metric the TFM seems to be superior because of the ability of the C/N_0 cancellation, the possibility of spoofing detection with no delay and spoofer movement detection for slow movements.

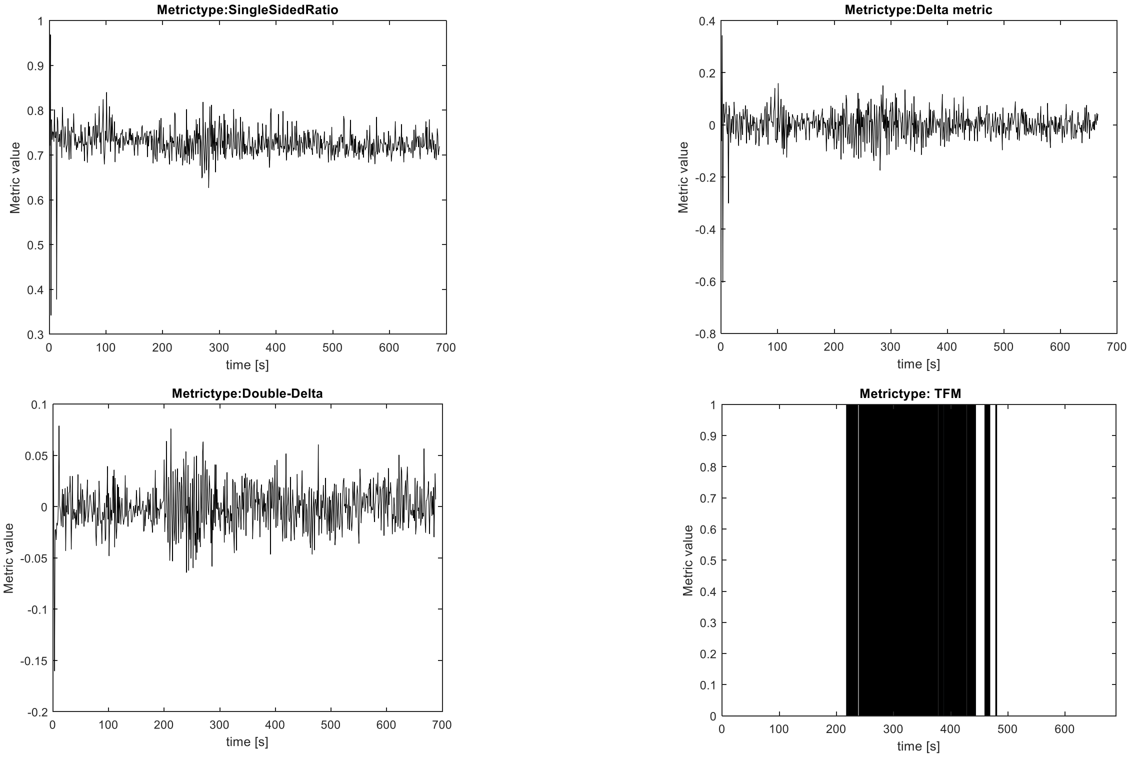

Figure 8: The metrics Single-Sided ratio, Delta, Double-Delta and TFM with the same correlator settings than in Figure 7 for a spoofing attack with a start delay of 0 m and a constant speed of 1 m/s, initialized at t=180 s. The authentic signal had a C/N_0 of 43 dBHz, the spoofing signal 48 dBHz. The spoofer used a gain of 5 dB in this case.

III.2 TFM results for real signals without spoofing

In Figure 9 the TFM is shown for real Galileo E1B satellite signals without spoofing, taken with a roof antenna at our institute. Several PRN's are plotted. If the bar's get the value 1, multipath is present, if 0 no multipath is present. Three satellite signals showed no multipath at all, two showed very few multipath and two showed a strong multipath occurrence (lower elevation angles). The spoofing alert (last plot) was always 0, which means, that no spoofing was present. The spoofing alert would go on, when all satellites have a TFM value changing from 0 to 1 at the same time. We analyzed several open sky data sets, where the spoofing alert was always 0, which shows the reliability of the TFM in open sky conditions. Note, that also GPS L1 C/A satellites were taken into account, therefore the number of satellites is on average much higher than 10, around 15 at our measurement site.

The metric however could fail against spoofer, which send all the signals each with a certain different delay or with multiple antennas, so that the signals reach the target at a different time. But it is not clear, if then the spoofing would be successful. This sort of attack is also much harder to realize and much more expensive, if many antennas would be used.

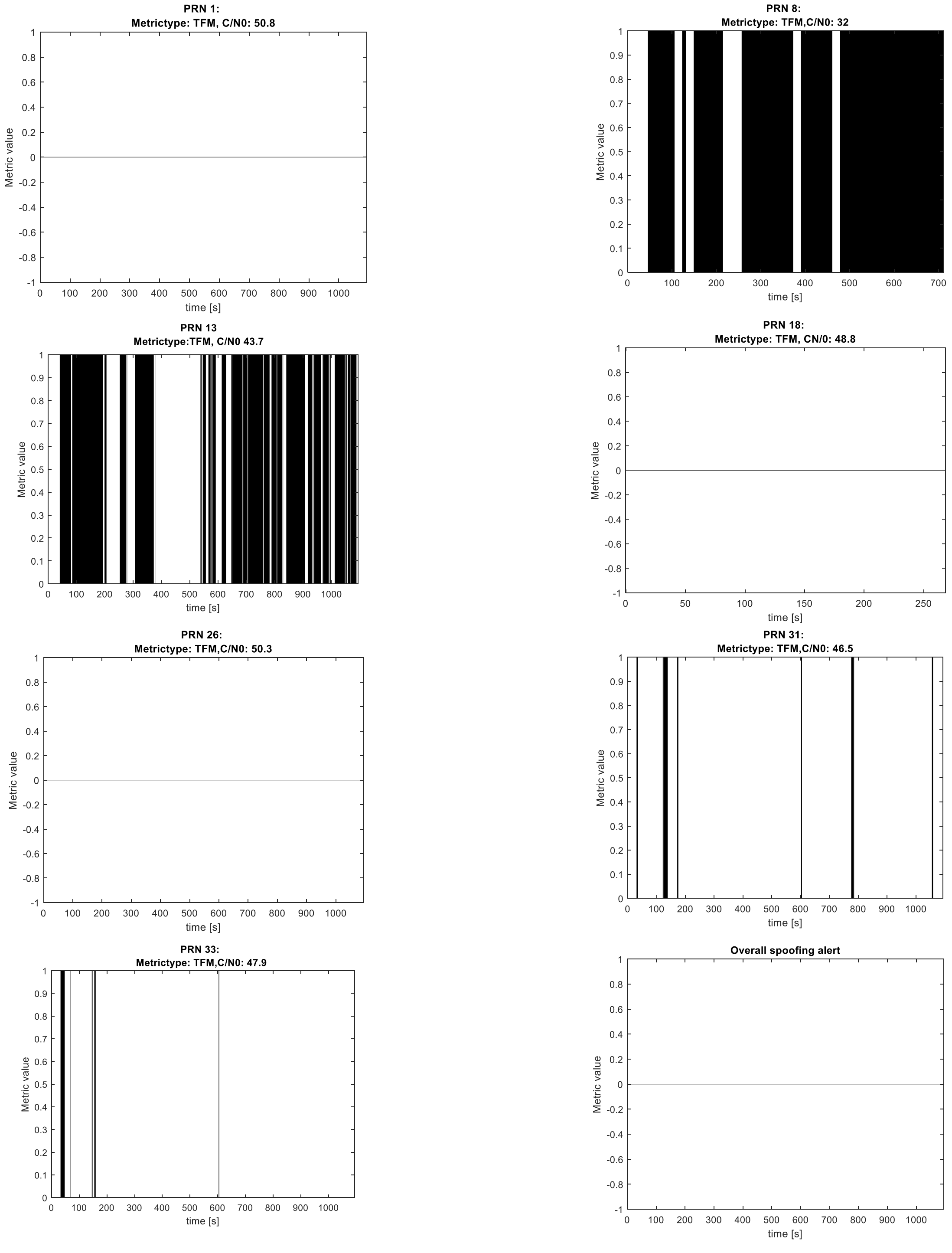

Figure 9: TFM for real satellite signals (here Galileo E1B) for several PRN's without spoofing. The signals were taken with a roof antenna, showing multipath, when the bar's get values of 1. 2 satellites show strong multipath, 3 no multipath and 2 few multipath. The overall spoofing alert was absent.

Since signals with lower C/N_0 values than 40 dBHz in general tend to have lots of multipath, one could also use only signals with C/N_0 values for example over 40 dBHz for spoofing detection to reduce the calculation time, maybe even over 45 dBHz if enough satellites can be tracked at the measurement site.

III.3 Signal generator attack results

The spoofer has to solve two major problems when spoofing real satellites. First, he has to set the gain in that way, that when his spoofing signal reaches the receiver, the power is higher than the authentic signal. We found out, that when the power is too high, the tracking often gets interrupted. This has to be avoided, since interruptions for all satellites for a static open sky scenario normally do not occur and are therefore noticeable. When the power is too low, the spoofing signal will not be tracked. The spoofer has to estimate the free space loss when transmitting over the air in order to get the right power.

A second point is the C/N$_0$. If the C/N$_0$ of the spoofer is similar than the C/N$_0$ of the authentic signal, we found out that fading effects occur more often, which can lead to tracking loss or a not successful spoofing. Therefore the spoofer must have a slightly higher C/N$_0$ value of 2-5 dB in order to get control of the receiver. Also the free space loss has to be estimated when transmitting over the air.

The LOKI spoofer has a delay (spoofing to authentic signal) setting, which however can only be set in 100 ns (30 m) steps. Therefore, it is not possible to set a continuous delay. This would be possible with an additional delay element. The smallest delay we could achieve with our specific cable setup, was around 15 m, which we found out in the CMC parameter in post-processing, which showed a jump of 15 m. In Figure 10, we see the metric results for the 15 m delay, a gain of 3 dB and a 3 dB higher C/N$_0$ for the authentic+spoofing signal compared to the authentic signal before the attack. The spoofing attack started at around 160 s. At around 220 s, the spoofer increased the delay with an acceleration of 0.1 m/s². Only the TFM and the Single Sided Ratio metric could significantly increase when the spoofing attack started in contrary to the Delta and Double-Delta metric, which showed a not so significant deviation at 160 s (also very noisy). At around 160 s, the TFM of all satellites (GPS L1 CA and Galileo E1B) switched from 0 to 1, which gave a spoofing alert in our receiver. Further experiments have to be made to confirm this behavior for other settings, for example other delays, gains etc. Also, further research has to be done to find out, why the delta and double delta metric could detect the attack in simulations, but not in the real attack over cable.

The initial position could be shifted away with the IFEN SX3, which shows that the spoofing worked. We also tested the spoofing attack with the U-Blox M8T and Septentrio PolaRx5TR with a spoofer gain of around 3 dB, also here both receivers could be spoofed (Figure 11 and Figure 12) and there was no spoofing alert in the U-Blox GUI of the software U-Blox center. Noticeable was, that the Septentrio could be spoofed with RAIM on and off, in both cases the position could be shifted away. However with RAIM on, there occurred some PVT losses during the attack because of the deteriorated pseudorange accuracy due to the overlap of spoofing and authentic signal. Also at this point it should be mentioned, that there were no obvious significant position or time jumps, which often occur for example for the Record and Replay attack. Also other parameters like the Code Minus Carrier or the Doppler showed no obvious jump behavior.

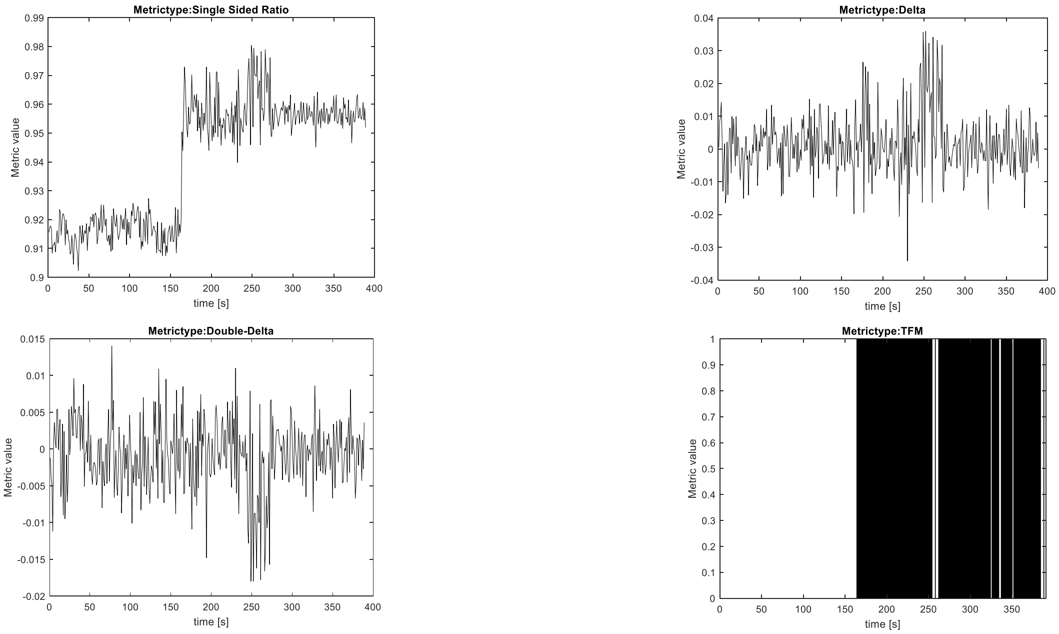

Figure 10: LOKI over the cable result for the Single Sided Ratio-, Delta-, Double-Delta- and TFM for Galileo E1B PRN 27. The spoofing attack started at around 160 s. The spoofer power gain was around 3 dB and the C/N$_0$ was adjusted, that the combination of spoofing and authentic signal has a 3 dB higher C/N$_0$ than the authentic signal.

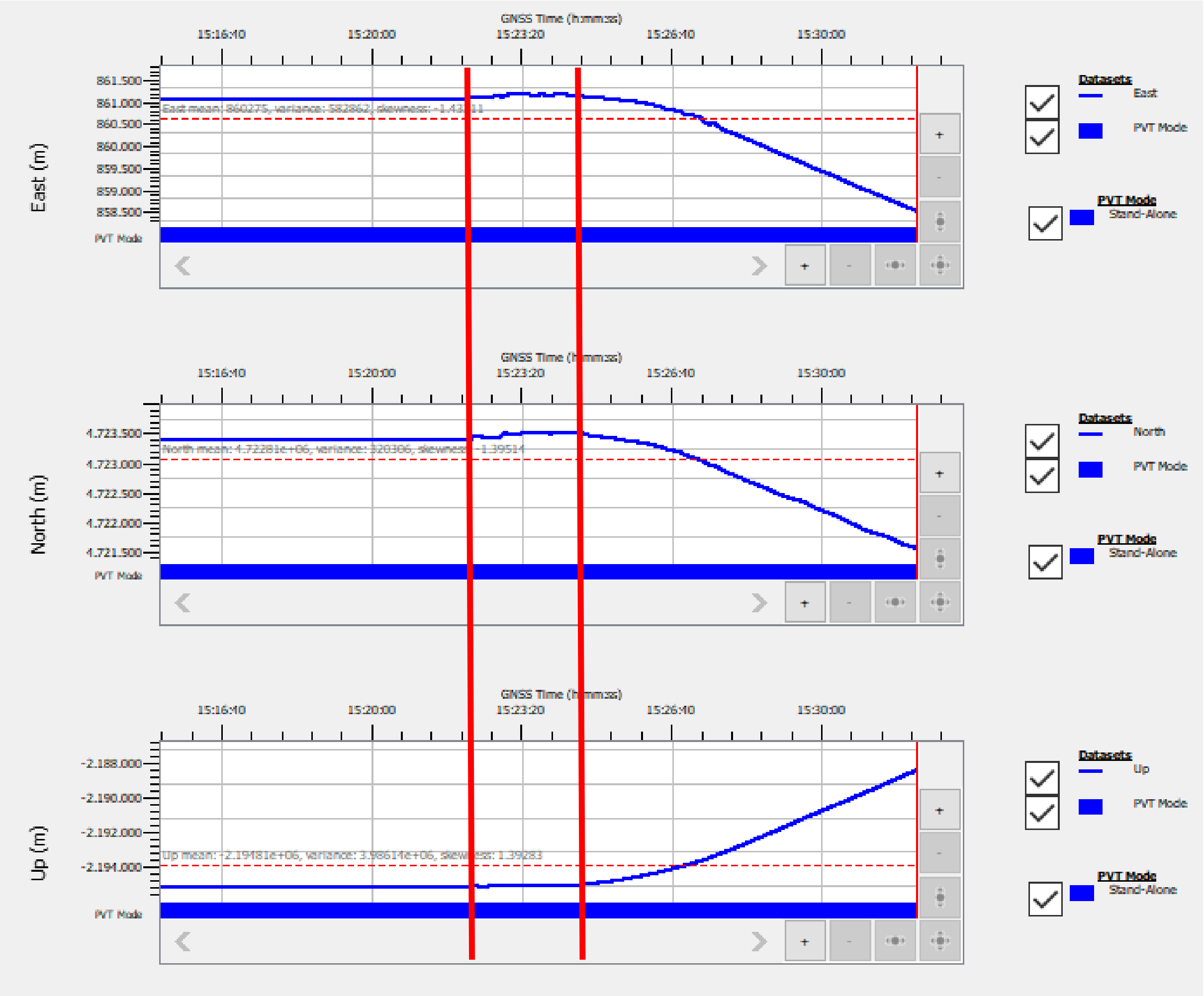

Figure 11: Relative ENU (East, North and Up) coordinates for the spoofing experiment with the Septentrio PolaRx5TR (RAIM off). The first red line indicates the spoofing start, the second one the start of the spoofer acceleration of 1 m/s². All position components showed the shifting.

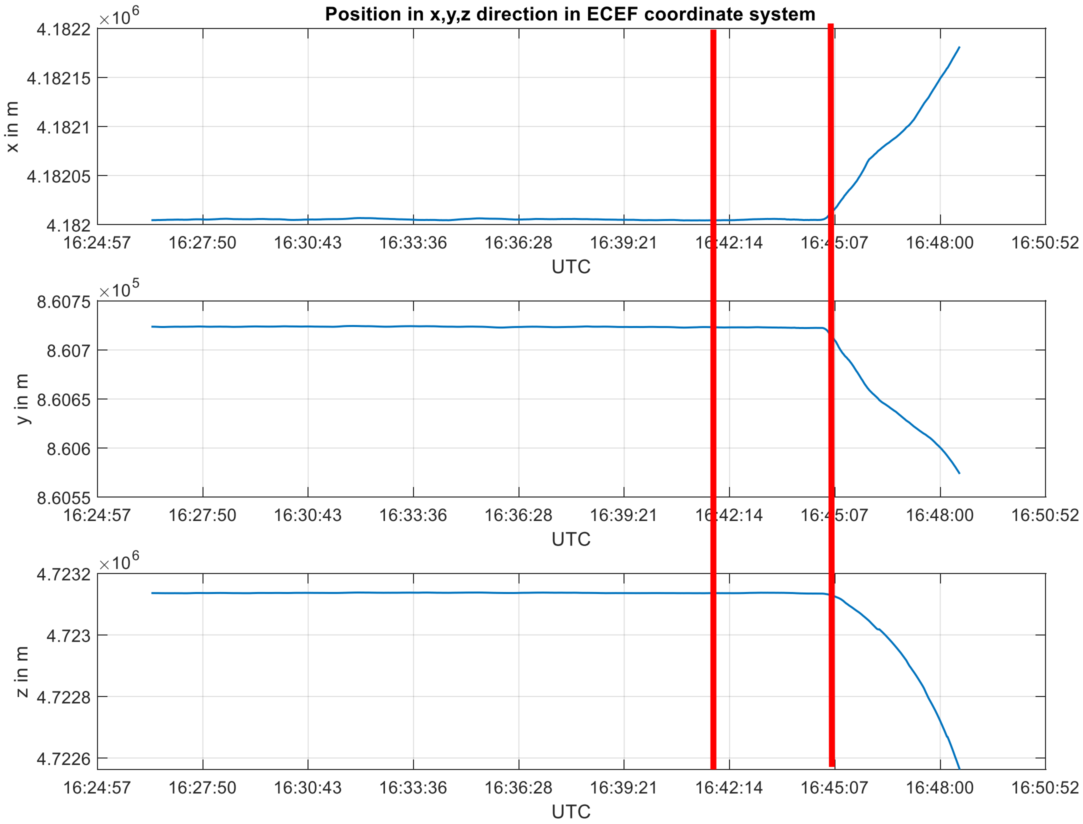

Figure 12: ECEF coordinate components X,Y and Z for the spoofing experiment with the U-Blox M8T. The first red line indicates the spoofing start, the second one the start of the spoofer acceleration of 1 m/s². All position components showed the shifting.

IV. CONCLUSIONS

We compared different SQM metrics in simulations and over the cable experiment. We found out in simulations, that the Single Sided Ratio, the Delta and the Double-Delta metric can give false alarms when the C/N_0 is changing immediately, which can happen due to shading or strong multipath. The self-designed TFM turned out to be robust against C/N_0 changing. In the simulations, the TFM could also detect 0 m delay attacks, when the spoofer increases the distance with a small speed, whereas the other metrics could not detect the attack, however this has to be further analyzed with further experiments. In the real attack over cable, the TFM could detect the attack for all satellites at the same time, also the Single-Sided ratio could detect the attack. The Delta and Double-Delta metric did not show a clear significant deviation when the attack started. At this point, we conclude that the TFM lead to a good detection performance against spoofing, and it has also a reduced false alarm rate compared to the other investigated metrics. The LOKI spoofer could shift the position away from the initial position for several receivers (IFEN SX3, U-Blox M8T and Septentrio PolaRx5TR). A weakness however is the delay setting, which can only be set in 100 ns steps. Further experiments with different spoofer settings will follow, also with other spoofing devices.

Funding:

The results presented in this work were developed within the project "GalileoFusion", 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).

V. REFERENCES

[1] 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.

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

[3] 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.

[4] 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.

[5] J. Bhatti and T. Humphreys, "Hostile control of ships via false GPS signals: demonstration and detection," *Navigation,* pp. 64(1): 51-66, 2017.

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

[7] P. Montgomery , T. Humphreys and B. Ledvina, "Receiver-autonomous spoofing detection: experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer," *Proceedings ION ITM 2009,* pp. 124-130, 2009.

[8] M. Berardo, E. Manfredini, F. Dovis and L. Presti, "A spoofing mitigation technique for dynamic applications," *8th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC),,* pp. 1-7, 2016.

[9] K. Wesson, B. Evans and T. Humphreys, "A combined symmetric difference and power monitoring GNSS anti-spoofing technique," *IEEE Global Conference on Signal and Information Processing,* pp. 217-220, 2013.

[10] A. Jovanovic, C. Botteron and P. Farine, "Multi-test detection and protection algorithm against spoofing attacks on GNSS receivers," *IEEE/ION Position, Location and Navigation Symposium - PLANS,* pp. 1258-1271, 2014.

[11] T. Gamba, M. Truong and B. Motella, "Hypothesis testing methods to detect spoofing attacks: a test against the TEXBAT datasets," *GPS solutions 21,* pp. 577-589, 2017.

[12] A. Cavaleri, B. Motella, M. Pini and M. Fantino, "Detection of spoofed GPS signals at code and carrier tracking level," *5th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC),* pp. 1-6, 2010.

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

[14] F. Dovis, X. Chen, A. Cavaleri, K. Ali and M. Pini, "Detection of Spoofing Threats by Means of Signal Parameters Estimation," *Proceedings of the 24th International Technical Meeting of the Satellite Division of The Institute of Navigation ION GNSS,* pp. 416-422, 2011.

[15] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen and G. Lachapelle, "GPS spoofer countermeasure effectiveness based on signal strength, noise power and C/N0 observables," *International Journal of Satellite Communications and Networking, vol.30,no.4,* pp. 181-191, 2012.

[16] D. Yuan, H. Li, F. Wang and M. Lu, "A GNSS Acquisition Method with the Capability of Spoofing Detection and Mitigation," *Chinese Journal of Electronics,* pp. vol. 27, no.1, 213-222, 2018.

[17] J. Parro-Jimenez, R. Ioannides, M. Crisci and J. Lopez-Salcedo, "Detection and mitigation of non-authentic GNSS signals: Preliminary sensitivity analysis of receiver tracking loops," *6th ESA Workshop on Satellite Navigation Technologies (Navitec 2012) & European Workshop on GNSS Signals and Signal Processing,* pp. 1-9, 2012.

[18] D. Shepard and T. Humphreys, "Characterization of Receiver Response to a Spoofing Attacks," *Proceedings of the 24th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS),* pp. 2608-2618, 2011.

[19] A. Broumendan, A. Jafarnia-Jahromi, G. Lachapelle and R. Ioannides, "An approach to siscriminate GNSS spoofing from multipath fading," *8th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC),,* pp. 1-10, 2016.

[20] E. Manfredini, F. Dovis and B. Motella, "Signal quality monitoring for discrimination between spoofing and environmental effects, based on multidimensional ratio metric tests," *Proceedings of the International Technical Meeting of The Institute of Navigation ION GNSS+,* 2015.

[21] M. Irsigler, "Multipath propagation, mitigation and monitoring in the light of Galileo and the modernized GPS," *Dissertation, Universität der Bundeswehr, Neubiberg,Germany,* 2008.

[22] R. Phelts, "Multicorrelator Techniques for Robust Mitigation of Threats to GPS Signal Quality," *Ph.D. Thesis, Stanford University, CA,* 2001.

[23] C. Sun, J. Cheong, A. Dempster, L. Demicheli, E. Cetin, H. Zhao and W. Feng, "Moving variance-based signal quality monitoring method for spoofing detection," *GPS Solutions. 2210.1007/s10291-018-0745-7,* 2018.

[24] E. Manfredini, D. Akos, Y. Chen, S. Lo, T. Walter and P. Enge, "Effective GPS Spoofing Detection Utilizing Metrics from Commercial Receivers," *Proceedings of the International Technical Meeting of The Institute of Navigation,* pp. 672-689, 2018.

[25] M. Pini, M. Fantino, A. Cavaleri, S. Ugazio and L. Presti, "Signal Quality Monitoring Applied to Spoofing Detection," *Proceedings of the 24th International Technical Meeting of the Sateliite Division of the Institute of Navigation (ION GNSS),* pp. 1888-1896, 2011.

[26] K. Ali, E. Manfredini and F. Dovis, "Vestigal signal defense through signal quality monitoring techniques based on joint use of two metrics," *IEEE/ION Position, Location and Navigation Symposium - PLANS,* pp. 1240-1247, 2014.

[27] K. Ali, X. Chen and F. Dovis, "On the use of multipath estimating architecture for spoofer detection," *International Conference on Localization and GNSS,* pp. 1-6, 2012.

[28] C. Sun, J. Cheong, A. Dempster, D. Zhao and W. Feng, "GNSS Spoofing Detection by Means of Signal Quality Monitoring (SQM) Metric Combinations," *Access IEEE, vol.6,* pp. 66428-66441, 2018.

[29] E. Manfredini, F. Dovis and B. Motella, "Validation of a signal quality monitoring technique over a set of spoofed scenarios," *7th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC),* pp. 1-7, 2014.

[30] A. Pirsiavash, A. Broumandan and G. Lachapelle, "Two Dimensional Signal Quality Monitoring for Spoofing Detection," *Proceedings of the ESA/ESTEC NAVITEC Conference,* pp. 14-16, 2016.

[31] Y. Yang, H. Li and M. Lu, "Performance Assessment of Signal Quality Monitoring Based GNSS Spoofing Detection Techniques," *China Satellite Navigation Conference (CNSC) Proceedings: Volume 1, 2015. Lecture Notes in Electrical Engineering, vol.340. Springer, Berlin, Heidelberg,* 2015.

[32] J. Huang, L. Presti, B. Motella and M. Pini, "GNSS spoofing detection: Theoretical analysis and performance of the Ratio Test metric in open sky," *ICT, Express, Vol.2, Issue 1,* pp. 37-40, 2016.

[33] M. Psiaki and H. Todd, "GNSS spoofing and detection," *Proceedings of the IEEE 104,* pp. 1258-1270, 2016.

[34] M. Fantino, A. Molino, P. Mulassano, M. Nicola and M. Rao, "Signal Quality Monitoring: Correlation mask based on Ratio Test metrics for multipath detection," *Proceedings of IGNSS Symposium,* 2009.

[35] J. Dampf, T. Pany, W. Bär, J. Winkel, L. Mervart, J. Rodriguez and R. Ioannides, "Real World Spoofing Trials and Mitigation," *Inside GNSS,* May 2017.