THE JOURNAL OF NAVIGATION (2020), **73**, 1052–1068. © The Royal Institute of Navigation 2020
doi:10.1017/S0373463320000168

Detection of Intermediate Spoofing Attack on Global Navigation Satellite System Receiver Through Slope Based Metrics

Abdul Malik Khan, Naveed Iqbal, Adnan Ahmed Khan, Muhammad Faisal Khan and Attiq Ahmad

(*National University of Sciences and Technology, Islamabad, Pakistan*)
(E-mail: amkhan.phd@students.mcs.edu.pk)

A spoofing attack on a global navigation satellite system (GNSS) receiver is a threat to a significant community of GNSS users due to the high stakes involved. This paper investigates the use of slope based metrics for the detection of spoofing. The formulation of slope based metrics involves monitoring correlators along with tracking correlators in the receiver's channel, which are slaved to the prompt tracking correlator. In this study, using some candidate metrics, detectors have been formed through the analysis of simulated spoofing attacks. A theoretical variance of each metric has also been calculated as a reference for the threshold. A threshold is estimated using the measured variance from the clean signals, for specific false alarm rate. By using the measured threshold, detectors are formed based on slope metrics. These detectors have been tested using TEXBAT data. The results show that the differential slope metrics have good performance. The results have also been compared with some other techniques of spoofing detection.

KEYWORDS

1. Spoofing. 2. Anti-spoofing. 3. Tracking Loop. 4. Signal Processing.

Submitted: 25 September 2018. Accepted: 1 March 2020. First published online: 3 April 2020.

1. INTRODUCTION.

Global navigation satellite systems (GNSS) are becoming a primary source of position, navigation and timing applications in a variety of fields and have a big user base (Ioannides et al., 2016; Psiaki and Humphreys, 2016). GNSS signals are vulnerable to environmental effects, interference, jamming and spoofing due to their low power and open signal structure (Juang, 2009; Huang et al., 2016). Navigation and timing services can be easily interrupted by interference or jamming, or misled by a spoofer through counterfeit signals. An intermediate spoofing attack that leverages a genuine signal in space to create counterfeit signals, transmitted from a single antenna, is the preferred method for the attacker because it does not break the receiver tracking loop lock on the signal and, as a result, does not panic the user. The spoofer produces a misleading signal that replicates the structure of an authentic signal to deceive the user. However, the basic problem for the spoofer is to break the lock of the user receiver tracking loop from the authentic signal and make it lock on the counterfeit signal generated by the spoofer, without alerting the user. In order to do this, the spoofer has to follow a sequence of initial operations to launch the intermediate spoofing attack (Humphreys et al., 2012). This sequence includes getting the signal parameters at user position, starting the attack by hiding the spoofing signal under the authentic signal and then dragging the spoofing signal away from the authentic signal to complete the attack (Humphreys et al., 2012).

The study of spoofing techniques and their mitigation is therefore an active area of study. Jafarnia-Jahromi et al. (2012) provide a classification of known spoofing techniques, while Ioannides et al. (2016) and Psiaki and Humphreys (2016) provide thorough coverage of spoofing attacks and mitigation techniques. Of many classes of technique discussed in Jafarnia-Jahromi et al. (2012), signal quality monitoring (SQM) is the one technique that has been used by many researchers including Cavaleri et al. (2010) and Ali et al. (2014). SQM techniques are effective during the phase of spoofing where the distortion due to the availability of the authentic and the counterfeit signal is significant. Likewise, there are other SQM techniques like delta metric, early-late phase metric, magnitude difference metric, etc. (Wesson et al., 2011). Each of these SQM techniques uses a combination of the correlator outputs or measurements and threshold/detection test to detect abnormality on account of multipath, spoofing, signal integrity, satellite failure, etc.

A set of SQM metrics based on normalised auto-correlation function (ACF) shape was proposed by Phelts et al. (2003). Here the author endeavoured to devise a reliable method for determining a set of SQM metrics for evil waveform detection. The paper describes a flexible, straightforward and quantitative approach to computing a set of highly-effective detection metrics, for the real-time SQM monitoring of the wide area augmentation system (WAAS) signal. The metrics described in the paper contain polynomial fit metrics that use the least squares method to fit linear and quadratic polynomials to the ACF. The method described in Phelts et al. (2003) for linear fit has been used to find the slope of the ACF in this study.

The present paper discusses a method based on slope metric that calculates the slope of ACF at the tracking point to obtain a signal quality metric that is sensitive to distortion in the ACF due to spoofing. The slope metric technique is based on the work of Townsend and Fenton (1994) and Phelts et al. (2003), which primarily addresses multipath and evil waveform detection issues. The technique uses normalised ACF for metric formulation. The normalisation of the measurement correlator using a tracking correlator is done in many SQM metrics (Pirsiavash et al., 2017). The normalisation by a tracking correlator gives an advantage in comparing the metric values. However, in fading channels when the direct signal is obstructed, such normalisation could lead to changes in the noise level of the signal (Alonso-Arroyo et al., 2017). Such situations may be detected by measuring the carrier to noise density ratio (C/N_0) of the signal and the decision-making process could be stopped when C/N_0 drops below a certain level.

The results of the slope based detector are compared with some recent studies in which the results are reported quantitatively (Wang et al., 2017; Wesson et al., 2018; Gross et al., 2019) and using the similar dataset in their studies. The spoofing detector reported by Wang et al. (2017) had a better detection rate than the proposed combination detector for only case 2 of TEXBAT; however, a complete comparison remains challenging because the numerical value of probability of false alarm (P_{FA}) is not reported in the results. Wesson et al. (2018) have given simulation results for their PD detector and the experimental results

https://doi.org/10.1017/S0373463320000168 Published online by Cambridge University Press

using TEXBAT cases except for case 7 where it uses a combination of symmetric difference metric and power measurement for classification of environment as clean, multipath, spoofing and jamming. Gross et al. (2019) improved upon the Wesson's work using the maximum-likelihood estimator to estimate the authentic signal parameters. It can be seen here that the combination detector performs equally well. If compared with legacy SQM detectors, etc. the proposed detector can easily outperform them, as these detectors use legacy tracking correlator outputs and Doppler measurement. Advanced spoofers, however, generate an attack in such a way as to disturb the Doppler and tracking correlator as little as possible and for a very short period of time.

The proposed method is found to be effective in the pull-off phase, which is the time when the delay between the spoofing and authentic signals is significant. The technique is also found to be effective in matched power as well as over-powered cases.

2. BACKGROUND.

A spoofer is a device capable of generating a signal similar to an authentic satellite signal that can deceive the victim receiver in such a way that it deduces an incorrect position, time or both. A detailed study of spoofing is presented below to understand how spoofing can be detected.

2.1. *Classification of spoofing attack.*

Spoofing attacks through the generation of satellite signals can be classified as simplistic, intermediate or sophisticated based on the complexity of the spoofer (Humphreys et al., 2008). A simplistic attack is conducted through a satellite simulator that is not synchronised to the current user environment. The intermediate and sophisticated spoofer uses a receiver to obtain the current satellite signal state and produce an output in synchronisation to the situation at the user receiver. An intermediate attack is launched through a single transmitter and can be detected through the angle of arrival discrimination methods. A sophisticated attack can be launched through multiple transmitters to overcome the victim's defences using the angle of arrival discrimination (Humphreys et al., 2008).

2.2. *Details of the intermediate attack.*

An intermediate spoofing attack uses a GNSS receiver to estimate the critical parameters, such as frequency, code phase and amplitude, during the alignment phase. These parameters are required in order to match the counterfeit and genuine signal, so that both signals appear as one in the target receiver correlation function. Separate parameters for each satellite are estimated to generate the data stream for each satellite. All data streams are combined and adjusted for power and then transmitted (Humphreys et al., 2012). After the alignment phase, the counterfeit signal power is increased to control the tracking loops of the target receiver. The counterfeit signal is then steered away from the authentic signal by changing the code phase (Humphreys et al., 2012). This process is called pull-off, and generates ACF distortion. When the pull-off phase is complete and the receiver is locked on the spoofed signal, away from the genuine signal, the phase is known as the capture phase. The spoofer now has complete control over the target receiver (Humphreys et al., 2008). Table 1 provides an overview of the spoofing sequence of each phase in the TEXBAT data (Humphreys et al., 2012).

2.3. *Dataset.*

To evaluate the slope metric publicly available datasets and independent field recordings were used.

2.3.1. *Spoofing dataset.*

The spoofing dataset was comprised of the TEXBAT dataset and the synthetic spoofing data (Khan et al., 2018). TEXBAT is the battery of recorded spoofing cases compiled by researchers at the University of Texas, Austin. It includes

Table 1. Phases of intermediate spoofing sequence and spoofing status.

Phase description	Spoofing status
Alignment: Spoofer sets the code and carrier phase according to the target position	Un-spoofed
Control: Spoofer increases the power to control the tracking loop, but does not steer it away	Spoofing starts
Pull-off: Spoofer drags the counterfeit signal away from the authentic signal	Spoofing
Capture: Spoofer hijacks the receiver	Spoofing

Table 2. Summary of TEXBAT cases.

Spoofing case description	Spoofer power advantage (dB)
1: Static Switch	N/A
2: Static Overpowered Time Push	10
3: Static Matched Power Time Push	1·3
4: Static Matched Power Position Push	0·4
5: Dynamic Overpowered Time Push	9·9
6: Dynamic Matched Power Position Push	0·8
7: Static Matched Power Time Push	N/A
8: Static Matched Power Time Push	N/A

clean static and dynamic cases and eight spoofing attack cases datasets. Table 2 provides a description of the spoofing cases and the spoofer power advantage. Spoofer power advantage is the ratio of the power of the spoofing signal to the authentic signal as seen by the target receiver. In order to generate spoofing cases, corresponding clean cases have been replayed using a vector signal generator (VSG). The output of the VSG has been split and one part is given to the receiver inside the spoofer to extract the required parameter and the other part is combined with the output of the spoofer to make the spoofing signal. The combined signal is recorded using vector signal analyser (VSA), with a bandwidth of 20 MHz, and digitised as complex 16-bit samples at a rate of 25 MSps (Humphreys et al., 2008).

2.3.2. *Non-spoofing dataset.* The non-spoofing dataset comprised of clean TEXBAT data, RNL Multipath War-drive data (Wesson et al., 2011), and data recorded in the field.

The RNL multipath and interference data contains static and dynamic cases in both light and dense urban environments around Austin, Texas. It exhibits mild-to-severe multipath and mild unintentional interference. The data is quantised in 16 bit and the recording is cantered at 1575·42 MHz (GPS L1) and at a complex sampling rate of 37 MSps.

The data acquired from the field consists of clean and multipath affected recordings using commercial satellite signal recorders. The signal recorders used have either MAX2769 Front-end, with complex sampling rate of 16·368 MSps, with IF of 4·092 MHz or NT1065 Front-end with sampling rate of 53 MSps, with IF of 14·58 MHz. The signal recorders were equipped with TCXO with an accuracy of about $\pm 5 \times 10^{-7}$ s/s. The data has been logged in clean, obstruction-free places as well as in urban places where high multipath and mild unintentional interferences were present.

2.3.3. *Pre-processing.* During the pre-processing phase, the data samples that have C/N_0 below 28 dB-Hz have been removed from the dataset, to avoid normalisation issues that may occur under low signal-to-noise ratio. The choice of minimum C/N_0 of 28 dB-Hz (Kaplan and Hegarty, 2005) eliminates most of the samples that can produce false alarm

https://doi.org/10.1017/S0373463320000168 Published online by Cambridge University Press

due to low signal strength while not affecting the detection in the receiver in tracking state under nominal conditions.

3. PROPOSED SLOPE BASED METRICS.

Quality monitoring is a process of measuring of the difference between the available or measured and the desired results. SQM techniques are based on either an observation of the measured ACF distortion or modelled characteristics of measured noise (Mitelman et al., 2000). The goal of slope based spoofing detection technique is to measure the signal quality by analysing the slope of ACF. A legacy receiver has three coherent tracking correlators for each channel. However, the SQM receiver uses additional monitoring correlators for computing metrics (Phelts et al., 2003). These monitoring correlators are linked to the tracking correlators and are at a specified distance from them. These monitoring correlators are used to measure slope metric value. Figure 1 depicts two different pairs of monitoring correlators along with tracking correlators. In the current section, a discussion on slope based metrics is presented.

3.1. *Mathematical model of ACF.*

After passing through the front-end and baseband section, a signal from a satellite, its reflection and the spoofing signal are accumulated for integration time, *T*. The accumulated value is an instantaneous measured ACF, given by

$$\begin{bmatrix} I_{\tau_i} \\ Q_{\tau_i} \end{bmatrix} = \sum_{n=0}^{N-1} \left[\sum_{\mathrm{s}} \mathrm{a_s} d(n+\tau_s) c(n+\tau_s) e^{j(2\pi f_{IF} n + \phi_s)} + \mathrm{N_o(n)} \right] c(n+\tau_i) e^{-j(2\pi f_{IF} n)}, \quad (1)$$

where subscript ‘s’ is used for different delayed versions due to spoofing or multipath and subscript ‘i’ is used for different correlators. $\mathrm{a_s}$ is amplitude of *s*th form of signal, $c(n)$ is locally generated replica PRN code and $e^{-j(2\pi f_{IF} n)}$ is the locally generated replica carrier, τ_i is the delay between locally generated code sequence and the received code for the *i*th correlator. $\tau_i = 0$ for the prompt correlator. N is the number of samples in integration time T and is defined as $N = f_c.\ T$, where f_c is the analog-to-digital conversion sampling rate. $e^{j(2\pi f_{IF} n)}$ is transmitted carrier, ϕ_s is transmitted carrier phase for *s*th version of signal, τ_s is the delay of *s*th signal from the direct signal.

After rearranging and simplification, the accumulated value in the in-phase branch of the correlator becomes

$$I_{\tau_i} = \sum_{s=0}^{M+1} \mathrm{a_s} \cos(\phi_s) R(\tau_i - \tau_s) + N_{\tau_i}, \quad (2)$$

where there are M multipath signals, a direct and a spoofing signal are assumed to be present, N_{τ_i} is the noise components after accumulation,$R()$ is an ideal ACF of GPS C/A code that is defined as

$$R(\tau) = \sum_{n=0}^{N-1} c(n) c(n-\tau), \quad (3)$$

The ideal ACF is approximately equal to the following (Kaplan and Hegarty, 2005)

$$R(\tau) = \left\{ \begin{matrix} \mathrm{N}\left[1 - \dfrac{|\tau|}{\mathrm{T_c}}\right] & \text{for } |\tau| \le \mathrm{T_c} \\ 0 & \text{otherwise} \end{matrix} \right\}, \quad (4)$$

The ideal ACF has the shape of a triangle as given in Figure 1.

https://doi.org/10.1017/S0373463320000168 Published online by Cambridge University Press

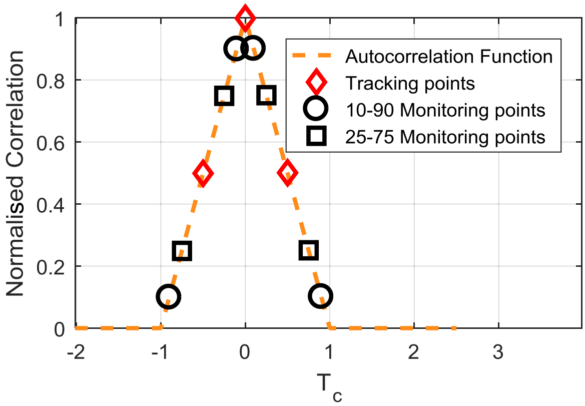

Figure 1. Tracking and monitoring correlators used to track and capture the slopes on a normalised ACF.

3.1.1. *Slope calculation.* Using the method given in Phelts et al. (2003), the slope of an ACF can be calculated using the least square method by solving the following equation, which estimates the slope (M_s) and y-intercept (I_y) in the least square sense

$$\begin{bmatrix} \tau_0 & 1 \\ \tau_1 & 1 \\ \tau_2 & 1 \end{bmatrix} \begin{bmatrix} M_S \\ I_y \end{bmatrix} = \begin{bmatrix} \tilde{\mathrm{I}}_{\tau_0} \\ \tilde{\mathrm{I}}_{\tau_1} \\ \tilde{\mathrm{I}}_{\tau_2} \end{bmatrix} \tag{5}$$

where $\tilde{\mathrm{I}}_{\tau_i} = \mathrm{I}_{\tau_i}$, τ_0, τ_1 and τ_2 are selected delays for calculating the slope.

However, if τ_1 is at the centre point between τ_0 and τ_2, it can be shown from Equation (5) that the slope can be calculated by the following equation

$$M_S(\tau_0, \tau_2) = \frac{\tilde{\mathrm{I}}_{\tau_2} - \tilde{\mathrm{I}}_{\tau_0}}{\tau_2 - \tau_0} = \frac{\mathrm{I}_{\tau_2} - \mathrm{I}_{\tau_0}}{\mathrm{I}_0[\tau_2 - \tau_0]} \tag{6}$$

where τ_0 and τ_2 can have any values and the τ_1 is the mean value of τ_0 and τ_2.

In order to understand the effect of multipath or spoofing, a direct and counterfeit signal is simulated with fixed spoofer power advantage and different time delays between the spoofing and authentic signal. The slope on the early and late side of the prompt tracking point is calculated using Equation (6). Figure 2 depicts the constituent signals ACF, the combined signal ACF, the tracking points and monitoring points at 25% and 75% of chip period (0·25T_c and 0·75T_c) on the ACF. The spoofer power advantage considered here is 0·8 dB corresponding to the matched power case. The tracking results are shown for delays of 0·2, 0·8 and 1·3 chips between the two signals. It can be observed that the slope value changes as the delay between the signal changes.

Figure 3 shows the same receiver parameters as shown in Figure 2, for the spoofer power advantage of 9 dB that corresponds to overpowered cases. It can be observed here that with such high spoofer advantage, there is little change in slope value of the measured ACF.

3.2. *Metric formulation.* The choice of placement of monitoring correlators is a critical factor in metric formulation. Noise will be enhanced if the monitoring correlators are very close to each other, because of the factor of $\tau_2 - \tau_0$ in the denominator of the Equation (6). To make a reasonable separation, the monitoring correlators used in this study are at 10%–90% and 25%–75% of the chip period.

https://doi.org/10.1017/S0373463320000168 Published online by Cambridge University Press

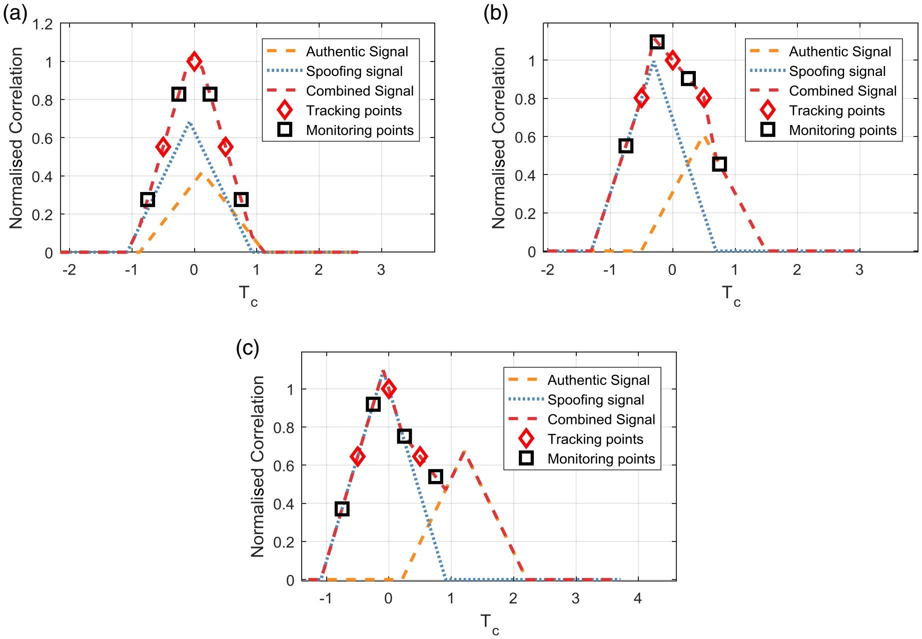

Figure 2. Slope of ACF at 25% and 75% of the tracked chips on both sides of the prompt tracking point, for spoofer power advantage of 0·8 dB: (a) the distortion in ACF is very low when the spoofing signal is 0·2 chip away from the authentic signal and slope values are not affected significantly, (b) spoofing signal is 0·8 chip away from the authentic signal due to which slope value has changed significantly, and (c) shows the spoofing signal as 1·3 chips away from the authentic signal due to which the slope value has changed drastically.

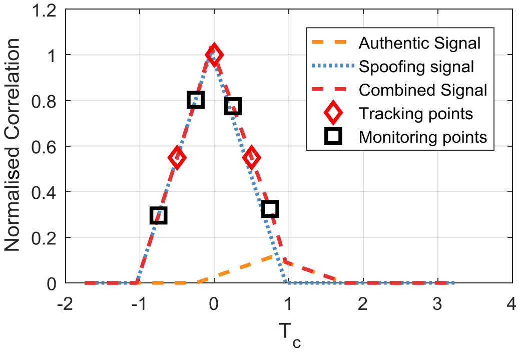

Figure 3. Slope of ACF between 25% and 75% of the tracked chips on both sides of the prompt tracking point, for spoofer power advantage of 9 dB and spoofing signal as 0·8 chips away from the authentic signal.

Equation (6) can be used to calculate early and late side slopes, where $M_s(-\tau_1, -\tau_0)$ produces early slope value and $M_s(\tau_1, \tau_0)$ produces late slope value for (τ_0, τ_1) monitoring correlators. In order to find an effective metric for spoofing detection, several metrics have been formulated consisting of slope metrics and the symmetric and asymmetric difference

https://doi.org/10.1017/S0373463320000168 Published online by Cambridge University Press

of slope metrics. The slope metrics are

$$\begin{aligned} M_{S1} &= M_S(0{\cdot}1, 0{\cdot}9) \\ M_{S2} &= M_S(-0{\cdot}1, -0{\cdot}9) \\ M_{S3} &= M_S(0{\cdot}25, 0{\cdot}75) \\ M_{S4} &= M_S(-0{\cdot}25, -0{\cdot}75) \end{aligned} \tag{7}$$

In order to create symmetric difference metrics from early and late pairs of slope measurement, their values are added in the following metric,

$$\begin{aligned} M_{D1} &= M_{S3} + M_{S4} \\ M_{D2} &= M_{S1} + M_{S2} \end{aligned} \tag{8}$$

where the M_{S1}–M_{S4} values are defined in Equation (7) and the M_{D1} and M_{D2} are symmetric differential slope metrics. The asymmetrical one-sided differential metrics can be formed by taking the difference of metrics on early or late sides as follows,

$$\begin{aligned} M_{D3} &= M_{S3} - M_{S1} \\ M_{D4} &= M_{S4} - M_{S2} \end{aligned} \tag{9}$$

where M_{D3} and M_{D4} are early and late side differential metrics. Considering the structure, the M_{D1} and M_{D2}metrics are similar to the double delta metric as described in Pirsiavash et al., (2017), except for the choice of monitoring correlators. However, M_{D3} and M_{D4} are novel in the sense that they use the one-sided monitoring correlators in metric formulation. The double delta metric is defined as follows:

$$M_{\mathrm{DT}} = \frac{(I_{-0{\cdot}1} - I_{+0{\cdot}1}) - (I_{-0{\cdot}05} - I_{+0{\cdot}05})}{I_0}.$$

Next, we calculate the nominal variation of the metrics that occurs due to the influence of thermal noise, as given in Irsigler (2008) for the slope metrics, given in Equations (7–9). Details of variance calculation are given in Appendix A.

Table 3 summarises the metrics and their variance for different C/N$_0$ values.

The variance calculated and presented in Table 3 is based on only the C/N$_0$ value of the signal. The values have been calculated here for the purposes of having a reference to the clean signal. The calculated variance may also be used as a sanity check on the calculated threshold.

In order to develop a metric suitable for the detection of a spoofing attack, we have simulated the spoofing attack scenario for a different power ratio between authentic and spoofer signal power. Slope metric values for different delays between authentic and spoofing signals are shown in Figures 4–6. Figure 4 contains the slope metrics (M_{S1}–M_{S4}) values. It can be noted here that the slope metric values change from their typical un-spoofed position (when $\Delta\tau = 0$) for even a very small change in the spoofing and authentic signal delay. Figure 5 contains the symmetrical differential slope metrics (M_{D1}, M_{D2}). The metrics have a low sensitivity (metric value does not change from the typical value) for small delays in the authentic and spoofing signals; however, they also have low sensitivity for the matched power cases. Figure 6 contains the asymmetrical one-sided differential slope metrics (M_{D3}, M_{D4}). It shows that there is very little change in the slope values for the small

https://doi.org/10.1017/S0373463320000168 Published online by Cambridge University Press

Table 3. Summary of slope based metrics, calculated statistics including expected value and variance formulas and values at different C/N_0.

Selected metric	Mean μ_m	Variance σ_m^2	Variance @ 28 dB-Hz $T = 1$ s	Variance @ 45 dB-Hz $T = 1$ s
M_{S1}	-1	$\dfrac{1.5}{2 \cdot C/N_0 \cdot T}$	0·0012	0·000023
M_{S2}	1			
M_{S3}	-1	$\dfrac{3}{2 \cdot C/N_0 \cdot T}$	0·00237	0·000047
M_{S4}	1			
M_{D1}	0	$\dfrac{12}{2 \cdot C/N_0 \cdot T}$	0·0095	0·00018
M_{D2}	0	$\dfrac{7 \cdot 5}{2 \cdot C/N_0 \cdot T}$	0·0059	0·00011
M_{D3}	0	$\dfrac{2 \cdot 065}{2 \cdot C/N_0 \cdot T}$	0·00163	0·000032
M_{D4}				
Double delta metric M_{DT}	0	$\dfrac{0 \cdot 2}{2 \cdot C/N_0 \cdot T}$	0·000025	0·000003

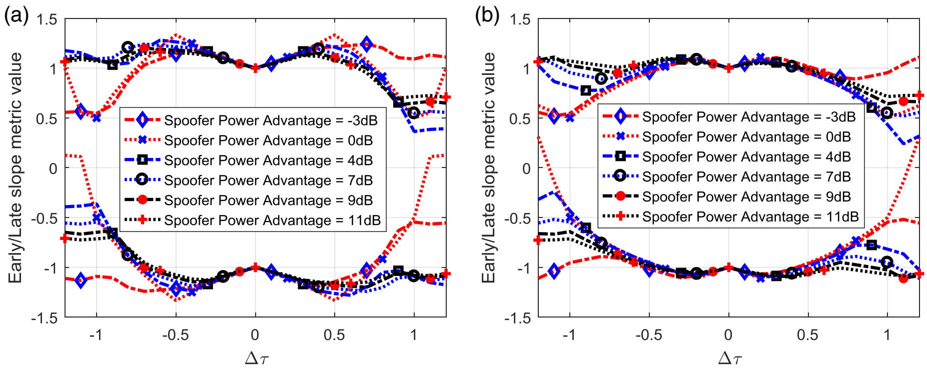

Figure 4. Slope value for monitoring correlators at (a) 25%–75% location at early and late side and (b) 10%–90% location at early and late side. Authentic and spoofing signals are simulated for different delay profiles and Spoofer Power Advantage.

delay between the authentic and spoofing signal, even if the power ratio varies. For the larger delays, however, the value of the slope changes considerably. This makes the choice of the asymmetrical one-sided difference slope metric more suitable for spoofing detection, as spoofing eventually has a large delay when the spoofer drags the signal away from the authentic signal (Humphreys et al., 2008).

3.3. *Threshold calculation.* A threshold for every metric is necessary for the detection process (Phelts et al., 2003). In order to calculate a reasonable threshold, statistical analysis has been performed to implement a Neyman Pearson (NP) detector. Here, we consider two hypotheses: the null hypothesis, H_0, which is considered when there is no spoofer present, and the alternate hypothesis, H_1, which is considered when the spoofer is present.

https://doi.org/10.1017/S0373463320000168 Published online by Cambridge University Press

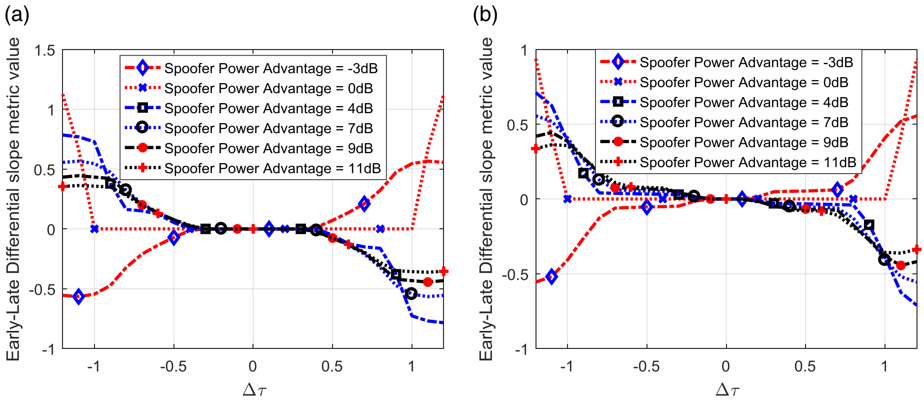

Figure 5. Symmetric differential slope metric values for monitoring correlators at (a) 25%–75% locations and (b) 10%–90% locations. Authentic and spoofing signals are simulated for different delay profile and spoofer power advantage.

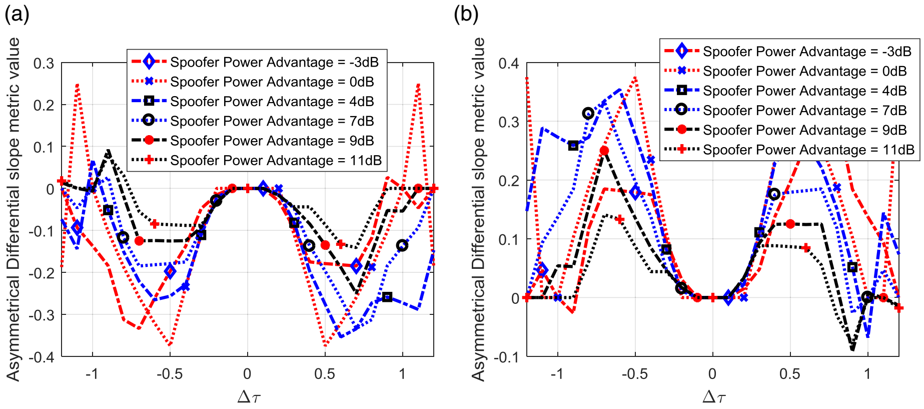

Figure 6. Non-symmetrical one-sided differential slope value for monitoring correlators at 10%–90% and 25%–75% location for (a) early correlators and (b) late correlators. Authentic and spoofing signals are simulated for different delay profiles and spoofer power advantage.

H_0: When the spoofer is not present, the correlation results contain power from an authentic signal, thermal noise, the multipath components, and other variations. Under the null hypothesis

$$H_0 : M_x \cong \mu_m \tag{10}$$

where M_x is any slope metric value and μ_m is its mean value.

H_1: When the spoofer is present, the correlation results contain the power from spoofing signal too. The expected value of the metric is changed under the spoofing, hence

$$H_1 : M_x \neq \mu_m \tag{11}$$

https://doi.org/10.1017/S0373463320000168 Published online by Cambridge University Press

In order to build an NP detector in the absence of completely defined distribution of alternate hypothesis, the likelihood function can be defined from Equations (10) and (11), as

$$\mathcal{L}(M_x) = |M_x - \mu_m| \tag{12}$$

Using the likelihood function, the P_{FA} for a given threshold γ can be calculated from the following,

$$P_{\mathrm{FA}}(\gamma) = \rho(|M_x - \mu_m| > \gamma | H_0) \tag{13}$$

where γ is the detection threshold, $\rho(\cdot)$ is the probability function and M_x is the desired slope based metric.

If P_{FA} is given, the detection threshold γ can be determined by inverting the probability function. As the slope based metrics are linear combinations of the accumulator outputs which are Gaussian (Huang et al., 2016; Pirsiavash et al., 2017), they are considered Gaussian with theoretical statistics given in Table 3, the threshold can be calculated using,

$$\gamma = \sqrt{2}\sigma_m erfc^{-1}(2 \cdot P_{\mathrm{FA}}) \tag{14}$$

where $erfc^{-1}$ is the inverse Gaussian function.

The probability of detection (P_D) or detection rate can be theoretically calculated by

$$P_D(\gamma) = \rho(|M_x - \mu_m| > \gamma | H_1) \tag{15}$$

As the statistical distribution of the disturbance due to the spoofing cannot be determined, however, an empirical solution for finding the detection rate has therefore been chosen in the results section, below.

3.4. *Spoofing detector.* Using the threshold, a statistical detector can be built from Equations (13) and (15)

$$|M_x - \mu_m| \underset{H_1}{\overset{H_0}{\lessgtr}} \gamma \tag{16}$$

A combination of metrics can also be used to form a detector. In this case Equation (16) can be used for detection using individual metrics and their detection results can be combined to achieve the final results, as below,

$$\begin{matrix} |M_{x_1} - \mu_{m_1}| > \gamma_1 \text{ or } |M_{x_2} - \mu_{m_2}| > \gamma_2 & \text{decide } H_1 \\ \text{otherwise} & \text{decide } H_0 \end{matrix} \tag{17}$$

where the subscripted values correspond to two different metric values and threshold.

4. RESULTS.

In order to gain an insight into slope based metrics, detectors based on the metrics listed in Table 3 and a combination detector have been considered for examination, using the datasets described previously. The non-spoofing datasets have been used for the P_{FA} calculation and the spoofing datasets have been used for calculation of P_D.

A software defined receiver (SDR) (Borre et al., 2006) with additional monitoring correlators has been used to generate tracking results. The integration time (T) has been selected as 1 s, whereas the correlation result is produced every 1 ms, and post-correlation integration for metric calculation has been carried out by coherent integrators. The SDR produces

Table 4. Results of slope metrics including calculated and measured thresholds and P_D for each case from TEXBAT and synthetic data for 0·1% P_{FA}.

Metric	γ_c	γ_m	P_D Case 2 [%]	P_D Case 3 [%]	P_D Case 4 [%]	P_D Case 5 [%]	P_D Case 6 [%]	P_D Case 7 [%]	P_D Case 8 [%]	P_D Synth [%]
M_{S1}	0·0145	0·09	0	27·76	45·97	0	10	69·67	92·43	0
M_{S2}	0·0145	0·11	0	8·36	44·97	0	31·72	55	72·43	8·45
M_{S3}	0·0207	0·09	3·34	40·80	73·15	0	10·69	65	92·43	0
M_{S4}	0·0207	0·11	89·30	77·26	26·51	0	30·69	64	91·89	5·63
M_{D1}	0·0415	0·064	0	23·41	57·05	1·03	33·1	64·67	91·89	9·86
M_{D2}	0·0328	0·064	0	20·74	30·87	0	40	69·33	92·43	11·27
M_{D3}	0·0172	0·017	96·66	76·92	94·63	97·9	97·6	70	92·43	92·25
M_{D4}	0·0172	0·028	96·66	92·31	94·63	99·32	96·9	68·67	92·43	39·44
M_{D43}	0·0172	0·028	96·66	93·65	95·3	99·32	98·62	70·67	92·33	93·66
M_{DT}	0·015	0·044	5·35	21·40	35·91	1·71	41·38	77·67	92·43	94·37

tracking and monitoring results every T seconds for each tracking channel. The value of each metric under study is calculated and a detection is considered if the metric value is greater than the threshold.

The study also includes a combination detector for the examination using M_{D3} and M_{D4}. The detector is formed as described by Equation (17). A single threshold for both constituent metrics has been used during the measurement of P_{FA} and P_D for the combination detector.

4.1. *Selection of threshold for specific* P_{FA}. To calculate the measured threshold (γ_m) for 0·1% P_{FA}, an arbitrary starting value of threshold is selected for each spoofing detection metric, for which detection is decided using Equation (16), using the data from the available set of satellites in non-spoofing cases. P_{FA} is calculated as the number of samples in which spoofing is detected out of total samples in which the spoofing is tested, which is effectively the averaging of detection in all satellites. The threshold value has been iteratively varied and a value is finally selected which gives the required P_{FA} of 0·1%. Before the detection process, the data samples that have C/N$_0$ below 28 dB-Hz have been removed from the dataset, to avoid normalisation issues that may occur under low signal-to-noise ratio. The measured threshold computed through the described method for each metric is given in Table 4.

The calculated threshold (γ_c) has been computed using Equation (14) for C/N$_0$ at 45 dB-Hz and P_{FA} of 0·1%. The C/N$_0$ has been chosen, based on the average carrier-to-noise ratio in the complete dataset. The result of the calculated threshold is also shown in Table 4.

4.2. *Measurement of* P_D. To calculate P_D, a non-spoofing dataset has been used. The measured threshold (γ_m) that produces specific P_{FA} is used in the detector. The spoofing period has been considered to be from the onset of spoofing until the end of the dataset, as given by the spoofing delay profile (spoofer delaying/advancing the spoofing signal compared with authentic signal) as described by Humphreys et al. (2012) and Lemmenes et al. (2016), and synthetic data delay profile as described by Khan et al. (2018).

By using the metrics values and employing Equation (16), the detection is declared for each measurement in each channel. The detection rate (P_D) has been calculated as the number of samples in which spoofing is detected out of total samples in which the spoofing is tested using measured threshold (γ_m), for each satellite, for each case listed in Table 2, effectively averaging the detection rate of all satellites. The detection rate (P_D) for each spoofing case is also listed in Table 4.

4.3. *Discussion of results.* The results of the experiments are summarised in Table 4 with thresholds and detection rates for each metric under study in different spoofing cases. It can be seen that the simple slope metrics, symmetric difference metrics, and the double delta metric could not perform well for spoofing detection. The measured threshold for these metrics is also found to be comparatively higher, showing that there are more nominal variations in these metrics. This indicates that these methods are more sensitive to the multipath and hence may be better suited for the multipath detection. On the other hand, the metric M_{D3} and M_{D4} (asymmetric one-sided differential metrics on early and late side) performed better with high detection rate for the same rate of false alarms. They also have a comparatively smaller threshold and a small difference between measured threshold (γ_m) and the calculated threshold (γ_c), suggesting that these metrics are less sensitive to the multipath and other nominal disturbances. It can also be observed that there is a difference between the detection rates of M_{D3} and M_{D4} metrics which is due to the pull-off direction of the spoofer. The spoofer always tries to adjust the pull-off direction of the spoofing signal such that the authentic signal appears as multipath. This may not be possible, however, in position-push cases where each satellite signal has to be steered such that a different position is deduced by the victim receiver and hence a different pull-off direction in some channels is necessary. Due to this fact, one metric has a higher detection rate than the other one. Therefore, the performance of a combination detector M_{D43} which uses the results of both metrics surpasses that of the other detectors.

It can also be observed that method M_{D43} performs better in case 2 and case 5 where the spoofer power advantage is very high. The high detection rate could be attributed to two phenomena. The first is the fact that the method is found good for even a very high spoofer advantage, as evident from Figure 6, which shows a significant metric value for different spoofer power advantages. Second, the overpowered cases are more similar to the multipath cases, but due to the random nature of multipath, and the inherent averaging in the method, it could differentiate between the multipath and spoofing. It can also be noted that case 2 and case 5 are time-push cases, which means that the spoofer delay profile is the same for all the channels, so detection is similar for each channel, which is not the case with position-push cases. Also in over-powered cases, the variation in signals due to spoofing starts early.

The results show that the slope based detector, when compared with some recent studies in which the results are reported quantitatively (Wang et al., 2017; Wesson et al., 2018; Gross et al., 2019), performs equally well. However, these methods require a larger number of correlators and a detector that is based on a complex detection procedure. On the other hand, the method proposed in this study uses a smaller number of monitoring correlators and the metric is composed of a simple linear combination of correlator value and detector output that is produced by applying a threshold. The structure of the slope metric based detector is therefore simpler than the comparable methods, and therefore it produces less computational burden. It is also evident from Table 4 that the double delta metric, whilst demonstrating good performance in detecting multipath (Irsigler, 2008), does not show a similar performance in the detection of spoofing.

In order to gain a complete insight into the performance of the detectors, the receiver operating characteristics (ROC) curve of selected detectors has been constructed and is given in Figure 7. For the purposes of building the ROC curve, the P_{FA} (using non-spoofing

https://doi.org/10.1017/S0373463320000168 Published online by Cambridge University Press

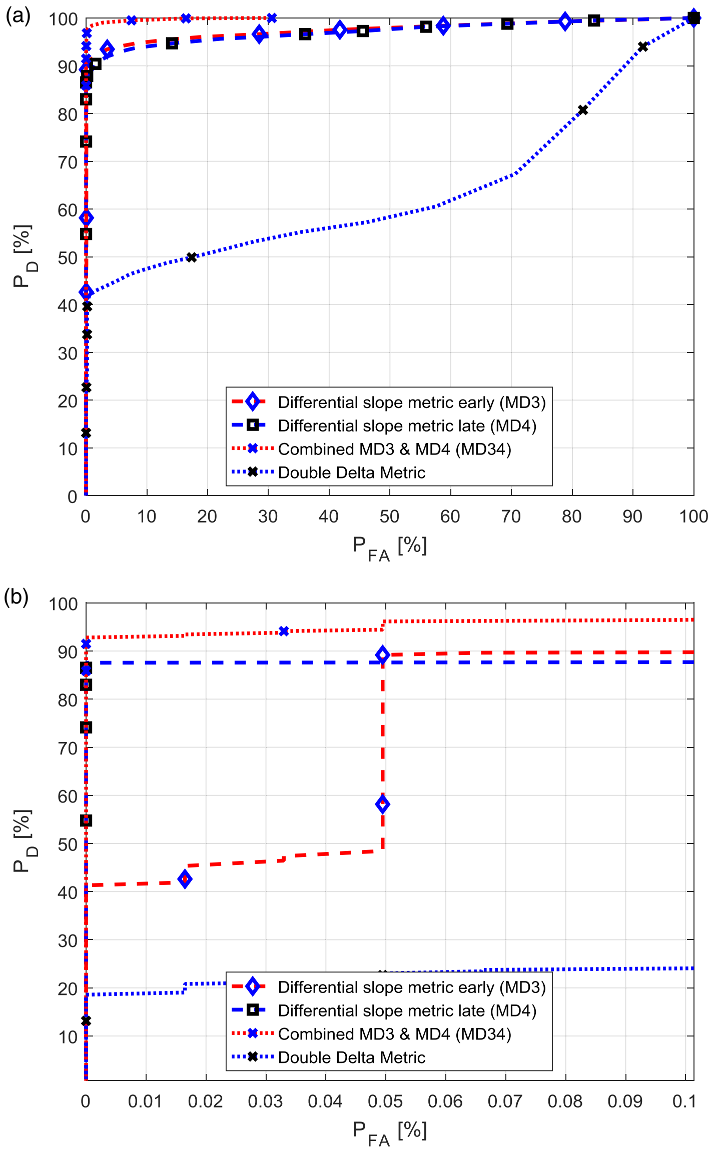

Figure 7. ROC curve of slope metric based detectors: (a) complete ROC (b) expanded view of ROC for performance comparison in low PFA.

dataset) and P_D values (using spoofing dataset) have been calculated and plotted as the threshold used in both calculations is varied simultaneously. The ROC curve is built by using the signals from all available satellites in the complete datasets used in this study. Looking into the ROC it can be seen that the Area Under the Curve (AUC), which is an important parameter in comparing detector performance, of the detector based on M_{D3} and M_{D4} is almost similar showing similar performance by them. However the AUC of the combination detector (M_{D43}) is much higher.

https://doi.org/10.1017/S0373463320000168 Published online by Cambridge University Press

Looking into the expanded view of the ROC curve it can be seen that the performance of the combination detector on the selected dataset is high for even a lower threshold value, suggesting that the threshold in the experiments can be further lowered with a very small decrease in detection rate but a significant decrease in false alarm rate.

5. CONCLUSION.

The study presented here has focussed on detecting spoofing attacks. This paper has proposed various slope based metrics for spoofing detection in intermediate/sophisticated spoofing attacks. The detectors based on asymmetrical differential slope metrics have been found to be robust and sensitive to spoofing attacks in matched power as well as overpowered cases as deduced from the simulation and demonstrated through experimental results. A combination detector based on two slope metrics has also been discussed in this paper and has been found to outperform other detectors. The combination detector has performed equally well in static and dynamic cases and on synthetically generated spoofing attacks. The detector performs better because of its sensitivity to the longer delay between authentic and spoofing signal, which can be attributed to spoofing. The double delta metric, well known for multipath detection, is also tested with the same method and found not to be suitable for spoofing detection, which may be attributed to the use of only legacy correlators. In most cases the distortions due to the spoofing do not affect the legacy correlators.

The slope metrics have been analysed in simulation and a theoretical variance of each metric has also been calculated that has been used as sanity check and can be used as a theoretical limit to the threshold. In the future, studies may be conducted to investigate the utilisation of more complex detectors and usage of the slope metric in multipath mitigation and other related studies.

REFERENCES

Ali, K., Manfredini, E. G. and Dovis, F. (2014). Vestigial Signal Defense Through Signal Quality Monitoring Techniques Based on Joint Use of Two Metrics. *IEEE/ION PLANS 2014*, Monterey, CA, 2014, pp. 1240–1247.

Alonso-Arroyo, A., Querol, J., Lopez-Martinez, C., Zavorotny, V. U., Park, H., Pascual, D., Onrubia, R. and Camps, A. (2017). SNR and standard deviation of cGNSS-R and iGNSS-R scatterometric measurements. *Sensors (Basel, Switzerland)*, 17(1), 183. http://doi.org/10.3390/s17010183

Borre, K., Akos, D., Bertelsen, N., Rinder, P. and Jensen, S. H. (2006). *A Software-Defined GPS and Galileo Receiver: Single-Frequency Approach*. Boston, MA: Birkhäuser.

Cavaleri, A., Motella, B., Pini, M. and Fantino, M. (2010). Detection of Spoofed GPS Signals at Code and Carrier Tracking Level. *2010 5th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC)*, Dec. 2010.

Gross, J. N., Kilic, C. and Humphreys, T. E. (2019). Maximum-likelihood power-distortion monitoring for GNSS-signal authentication. *IEEE Transactions on Aerospace and Electronic Systems*, 55(1), 469–475.

Huang, J., Lo Presti, L., Motella, B. and Pini, M. (2016). GNSS spoofing detection: theoretical analysis and performance of the Ratio Test metric in open sky. *ICT Express*, 2(1), 37–40.

Humphreys, T. E., Ledvina, B. M., Psiaki, M. L., O'Hanlon, B. W. and Kintner, P. M. (2008). Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer. *Proc. 21st International Technical Meeting of the Satellite Division of Institute of Navigation*, Savannah, Ga, September 16–19, pp. 2314–2325.

Humphreys, T. E., Bhatti, J. A., Shepard, D. P. and Wesson, K. D. (2012). The Texas Spoofing Test Battery: Toward a Standard for Evaluating GPS Signal Authentication Techniques. *Proceedings of the 25th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2012)*, Nashville, TN, September 17–21, pp. 3569–3583.

Ioannides, R. T., Pany, T. and Gibbons, G. (2016). Known vulnerabilities of global navigation satellite systems, status, and potential mitigation techniques. *Proceedings of the IEEE*, 104(6).

https://doi.org/10.1017/S0373463320000168 Published online by Cambridge University Press

Irsigler, M. (2008). Multipath propagation, mitigation and monitoring in the light of Galileo and modernized GPS. Ph.D. dissertation, University of Federal Armed Forces, Munich, Germany.

Jafarnia-Jahromi, A., Broumandan, A., Nielsen, J. and Lachapelle, G. (2012). GPS vulnerability to spoofing threats and a review of antispoofing techniques. *International Journal of Navigation and Observation*, 2012, 16 pages. Article ID 127072.

Juang, J. C. (2009). Analysis of global navigation satellite system position deviation under spoofing. *IET Radar, Sonar & Navigation*, 3(1), pp. 1–7.

Kaplan, E. D. and Hegarty, C. J. (ed) (2005). *Understanding GPS: Principles and Applications.* 2nd ed., Boston/London: Artech House, 2005.

Khan, A. M., Iqbal, N. and Khan, M. F. (2018). Synthetic GNSS spoofing data generation using field recorded signals. *MethodsX*, 5, 1272–1280.

Lemmenes, A., Corbell, P. and Gunawardena, S. (2016). Detailed Analysis of the TEXBAT Datasets Using a High Fidelity Software GPS Receiver. *Proceedings of the 29th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2016)*, Portland, OR, September 2016.

Mitelman, A. M., Phelts, E., Akos, D. M., Pullen, S. P. and Enge, P. K. (2000). A Real-Time Signal Quality Monitor for GPS Augmentation Systems. *Proceedings of the 13th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS 2000)*, Salt Lake City, UT, September 19–22, 2000, pp. 862–871.

Phelts, R. E., Walter, T. and Enge, P. (2003). Toward Real-Time SQM for WAAS: Improved Detection Techniques. ION GPS/GNSS 2003, 9–12 September 2003, Portland, OR.

Pirsiavash, A., Broumandan, A. and Lachapelle, G. (2017). Performance Evaluation of Signal Quality Monitoring Techniques for GNSS Multipath Detection and Mitigation. *International Technical Symposium on Navigation and Timing (ITSNT) 2017, ENAC*, Toulouse, France, Nov14–17, 2017.

Psiaki, M. L. and Humphreys, T. E. (2016). GNSS spoofing and detection. *Proceedings of the IEEE*, 104(6), 1258–1270.

Townsend, B. and Fenton, P. (1994). A Practical Approach to the Reduction of Pseudorange Multipath Errors in a L1 GPS Receiver. *Proceedings of the 7th International Technical Meeting of the Satellite Division of the Institute of Navigation, ION-GPS 94*, September 20–23, 1994, Salt Lake City, Utah, pp. 143–148.

Wang, F., Li, H. and Lu, M. Q. (2017). GNSS spoofing detection and mitigation based on maximum likelihood estimation. *Sensors*, 17(7), 1532; https://doi.org/10.3390/s17071532.

Wesson, K. D., Shepard, D. P., Bhatti, J. A. and Humphreys, T. E. (2011). An Evaluation of the Vestigial Signal Defense for Civil GPS Anti-Spoofing. *Proceedings of the 24th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2011)*, Portland, OR, September 2011, pp. 2646–2656.

Wesson, K. D., Gross, J. N., Humphreys, T. E. and Evans, B. L. (2018). GNSS signal authentication via power and distortion monitoring. *IEEE Transactions on Aerospace and Electronic Systems*, 54(2), 739–754.

APPENDIX A. METRIC VARIANCE CALCULATION

To calculate variance due to noise in the slope metrics (M_{S1}–M_{S4}) of a form $((I_{\tau_2} - I_{\tau_1})/(|X - Y|\, I_{\tau_0}))$ as given in Equation (6) following the equation from Irsigler (2008) can be used

$$\sigma_m = \frac{2R(\tau_0)[1 - R(\tau_2 - \tau_1)] + [R(\tau_2) - R(\tau_1)][2R(\tau_1 - \tau_0) - 2R(\tau_2 - \tau_0) + ((R(\tau_2) - R(\tau_1))/(R(\tau_0)))]}{2(\tau_2 - \tau_1)^2 CNo \cdot T \cdot R^3(\tau_0)} \tag{A1}$$

where τ_2, τ_1 and τ_0 are the relative delay of the in-phase measurement correlator in reference of prompt correlator, i.e. $\tau_0 = 0$, $R()$ is the autocorrelation function, CN_0 is the carrier-to-noise ratio and T is the integration time.

For the differential slope metric (M_{D1}–M_{D4}), which generally has a form $((I_{\tau_2} - I_{\tau_1})/(|\tau_2 - \tau_1|I_{\tau_0})) - ((I_{\tau_4} - I_{\tau_3})/(|\tau_4 - \tau_3|I_{\tau_0}))$, the variance can be also calculated by using the method given in Irsigler (2008). Using the referenced method, the variance can be calculated from the following equation

$$\sigma_m = \frac{ADA^T}{2 \cdot CNo \cdot T} \tag{A2}$$

where

$$A = \left[\frac{1}{|\tau_2 - \tau_1|R(\tau_0)} \frac{-1}{|\tau_2 - \tau_1|R(\tau_0)} \frac{1}{|\tau_4 - \tau_3|R(\tau_0)} \frac{-1}{|\tau_4 - \tau_3|R(\tau_0)} \frac{R(\tau_2 - \tau_1)}{|\tau_2 - \tau_1|R^2(\tau_0)} - \frac{R(\tau_4 - \tau_3)}{|\tau_4 - \tau_3|R^2(\tau_0)}\right]$$

$$D = \begin{bmatrix} 1 & R(\tau_2 - \tau_1) & R(\tau_2 - \tau_4) & R(\tau_2 - \tau_3) & R(\tau_2 - \tau_0) \\ R(\tau_1 - \tau_2) & 1 & R(\tau_1 - \tau_4) & R(\tau_1 - \tau_3) & R(\tau_1 - \tau_0) \\ R(\tau_4 - \tau_2) & R(\tau_4 - \tau_1) & 1 & R(\tau_4 - \tau_3) & R(\tau_4 - \tau_0) \\ R(\tau_3 - \tau_2) & R(\tau_3 - \tau_1) & R(\tau_3 - \tau_4) & 1 & R(\tau_3 - \tau_0) \\ R(\tau_0 - \tau_2) & R(\tau_0 - \tau_1) & R(\tau_0 - \tau_4) & R(\tau_0 - \tau_3) & 1 \end{bmatrix}$$

where the τ_1, τ_2, τ_3, and τ_4 are the relative delays of measurements with reference to the reference correlator τ_0.

https://doi.org/10.1017/S0373463320000168 Published online by Cambridge University Press