GNSS Spoofing Detection Using Moving Variance of Signal Quality Monitoring Metrics and Signal Power

Lixuan Li, Chao Sun(✉), Hongbo Zhao, Hua Sun, and Wenquan Feng

Beihang University, Beijing 100191, China
sunchao@buaa.edu.cn

Abstract. Spoofing represents a significant threat to the integrity of applications relying on Global Navigation Satellite System (GNSS). A spoofer transmits counterfeit satellite signals to deceive the operation of a receiver. As multipath and spoofing signals have similar signal structures, Signal Quality Monitoring (SQM) techniques, originally designed for multipath detection, were identified to be useful for spoofing detection. Recently, a moving variance (MV) based SQM method was developed to improve the performance of raw SQM metrics. However, the main problem with implementing the MV-based SQM technique is differentiating the spoofing attack from multipath. This work presents a two-dimensional detection method using carrier power and moving variance to improve detection performance. Besides, false alarms caused by multipath are avoided by the two-dimensional threshold. A dataset called Texas Spoofing Test Battery and a multipath scenario from Osaka were employed to evaluate the performance of the proposed algorithm.

Keywords: Moving variance · Carrier power · Spoofing · Signal quality monitoring

1 Introduction

Global Navigation Satellite System (GNSS) provides accurate positioning and timing services and is therefore used widely in various fields including civil aviation, mapping, maritime, military reconnaissance and finance. Despite the advantages of continuous and real-time working, GNSS is vulnerable to intentional as well as other types of interference due to its low signal power, and poor channel conditions.

Spoofing, studied in this work, represents one of the intentional interferences mentioned above and involves transmitting counterfeit satellite signals to deceive the target receiver into obtaining the wrong position results. It is worth mentioning that this kind of attack is often hidden and difficult to perceive. Therefore, in recent years, with the recognition of the danger of spoofing attacks, some researches have focused on their detection.

H. Gao et al. (Eds.): ChinaCom 2019, LNICST 312, pp. 537–548, 2020.
https://doi.org/10.1007/978-3-030-41114-5_40

The similarity between the complex correlation functions of counterfeit and multipath signals which sees them both delayed with varying phases of the authentic signal (also LOS in terms of multipath vocabulary), has attracted the attention of several research groups [1–3]. These groups have suggested that signal quality monitoring (SQM) techniques designed for multipath signals can also be used for the detection of spoofing. These SQM techniques consist in metrics computed from correlator outputs with their performances studied for multipath, as well as spoofing detection [2–5]. On this basis, Ali Pirsiavash et al. proposed a two-dimensional SQM method. However, the performance of the metrics proposed by these technologies is purely dedicated to detecting fraudulent signals and lacks the ability to distinguish the effects when there is an existence of multipath signals. On the other hand, power and carrier-to-noise ratio have also been used to detect spoofing signals [6]. In addition, Kyle D. Wesson et al. proposed power and distortion monitoring methods [7].

Recently, a SQM method using moving variance has been proposed and behaves superior in the detection of the onset of a frequency unlocked spoofing attack [8], which still lacks discussion of multipath conditions. To improve the detection performance of the moving variance method, we additionally use carrier power for two-dimensional observation. On the basis of this, the work further proposes a time threshold detection technique to help distinguish spoofing from possible multipath signals while detecting these attacks.

2 Spoofing Pattern

Spoofer aims at all the visible satellite signals of the target receiver and tracks each one to obtain the navigation and timing data corresponding to the authentic signal, Fig. 1b (1), so that it is able to generate counterfeit signals with the same code delay and Doppler shift as the legitimate signals.

Subsequently, the authentic satellite and broadcast spoofing signals simultaneously arrive at the receiver antenna, indicating the beginning of a spoofing attack.

To ensure the success of the spoofing attack, the two kinds of signals' complex correlation functions have to be aligned and the power of the generated signal must initially be at a low level.

However, spoofer slowly increases the power until it exceeds the authentic one, Fig. 1b (2). As a result, the receiver starts tracking fake signals the next moment, which means that the spoofer gains control of the tracking loop. After that, the tracking loop is further guided till it is removed from the legitimate signal, Fig. 1b (3).

In this way, spoofing attacks can be covertly carried out while the victim still be-lieves that the obtained position and timing information is derived from authentic signals.

Two different kinds of spoofing attacks are to be distinguished:

- named Matched-Power spoofing attack [1] in this paper they are sophisticated attacks where the spoofer attempts to closely match the power of the authentic signals.
- named Overpowered spoofing attack [1] in this paper they are sophisticated at-tacks where the spoofer eclipses the power of the authentic signals.

Once the spoofing signal is broadcast, Fig. 1b (2), the receiver obtains a mixed signal comprising authentic and counterfeit signals.

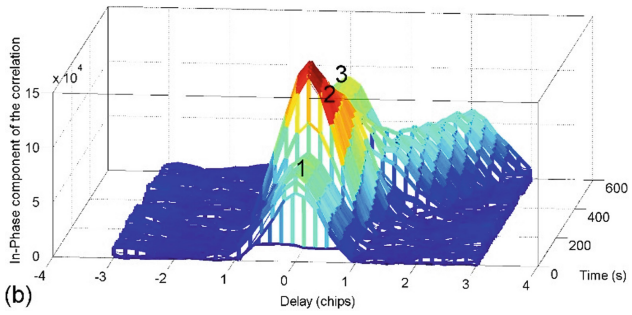

Fig. 1. In Phase component of a signal complex correlation function under no-spoofing circumstances (a) and assuming a spoofing attack (b).

The total received signal presented in Fig. 2 comprises a Line of Sight GPS signal, a spoofing component; some multipath components and additive noise which we assumed to be additive white Gaussian noise in this study.

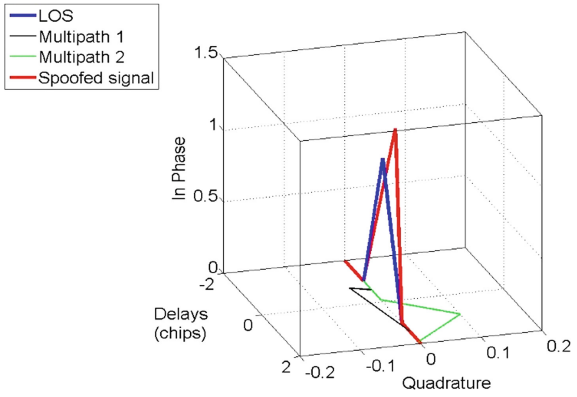

Fig. 2. The theoretical signals admixture model during the interaction step of the spoofing attack [2].

3 Signal Generation and Detection Metrics

3.1 Scenario

The Radio navigation Laboratory at the University of Texas provided a dataset of scenarios collections, known as the Texas Spoofing Test Battery (TEXBAT), for the analysis of the performance of the metrics with regard to spoofing detection. In addition, signals tracking is implemented by a GPS software receiver.

Under the assumption of no spoofing attacks, TEXBAT includes records of both static and dynamic GPS signals, with the same records being presented in Table 1 in six different spoofing scenarios. In all the scenarios, the spoofing attack begins approximately on the 100th second and the total record duration is 420 s.

Table 1. Texas Spoofing Test Battery: Scenarios Summary [1].

Scenario description	Spoofing type	Platform mobility	Power adv.(dB)	Frequency lock
1: Static switch	N/A	Static	Unlocked	Unlocked
2: Static overpowered	Time	Static	10	Unlocked
3: Static matched-power	Time	Static	1.3	Locked
4: Static matched-power	Position	Static	0.4	Locked
5: Dynamic overpowered	Time	Dynamic	9.9	Unlocked
6: Dynamic matched-power	Position	Dynamic	0.8	Locked

In addition, a multipath environment scenario recorded as a drive in Osaka, Japan, was used to supplement the TEXBAT datasets. It was provided by the set of examples available on the LabSat hardware. The data corresponded to GNSS signals and was post processed using the receiver software, NordNav.

Hence, the work had been run on GPS L1 C/A signals only.

3.2 Signal Quality Monitoring Metric

Signal Quality Monitoring performances have been studied and detailed in [3]. Their formulas are presented below.

In this paper, δ represents the Early-Late spacing and the correlator spacing was called the actual δ/2 spacing used between the prompt correlator and the Late and Early ones, respectively ahead and behind.

Delta. The Delta Metric $\Delta_{\delta(t)}$ is defined as [2].

$$\Delta_{\delta(t)} = \frac{I_{E,\delta(t)} - I_{L,\delta(t)}}{2 * I_P} \tag{1}$$

Ratio. The Ratio Metric $RT_{\delta(t)}$ is defined as [2].

$$RT_{\delta(t)} = \frac{I_{E,\delta(t)} + I_{L,\delta(t)}}{2 * I_P} \tag{2}$$

Early Late Phase. The Early-Late Phase Metric $ELP_{\delta(t)}$ is defined as [2].

$$ELP_{\delta(t)} = tan^{-1}\left(\frac{Q_{L,\delta(t)}}{I_{L,\delta(t)}}\right) - tan^{-1}\left(\frac{Q_{E,\delta(t)}}{I_{E,\delta(t)}}\right) \tag{3}$$

Magnitude Difference Metric. The Magnitude Difference Metric $MD_{\delta(t)}$ is defined as [2].

$$MD_{\delta(t)} = \frac{|x_{E,\delta(t)}| - |x_{L,\delta(t)}|}{2 * |x_P|} \tag{4}$$

3.3 Metric Responses to Spoofing and Multipath

Figure 3 shows the typical profile of metric responses to a spoofing attack. There is a progressive rising and declivity of the metric values during the second step with the interactions of authentic and counterfeit signals occurring between the 180th and the 280th seconds. For the first and third steps, when the authentic signal or the counterfeit signal is tracked, before the 150th second and after 280th seconds respectively in Fig. 3, the values keep a steady behavior overall.

Significant metric variations occurred at the second stage, making the SQM-based spoofing detection method feasible. These metric fluctuations were due to the variations of the correlator outputs caused by the distortion of the mixed signals' correlation function.

However, it is worth noting that large variations were observed for the Matched-Power spoofing attack while weaker ones occurred for the Overpowered attack because the interaction during the latter scenario is less than that in the former.

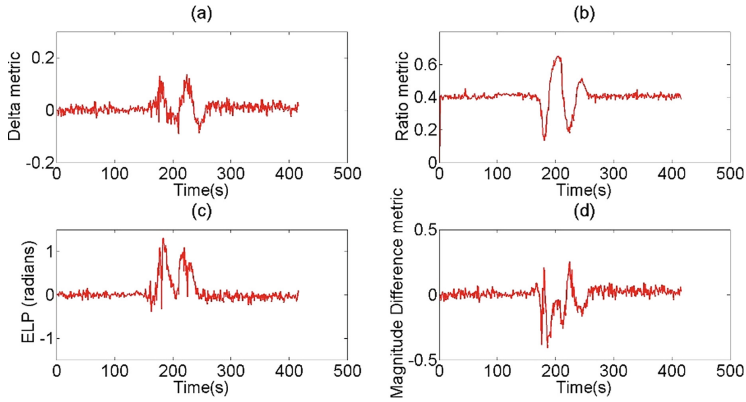

Fig. 3. The four metric responses: (a) Delta (b) Ratio (c) ELP (d) Magnitude Difference to a Matched-Power spoofing scenario: scenario 6 from TEXBAT and computed with a 0.56 chip correlator spacing.

Different from spoofing, metric responses to multipath have random peaks, as shown in Fig. 4. Nonetheless, the metric values vary within the same amplitude range in both

conditions, which may lead to false alarms when using the method of a threshold on metric values to detect spoofing.

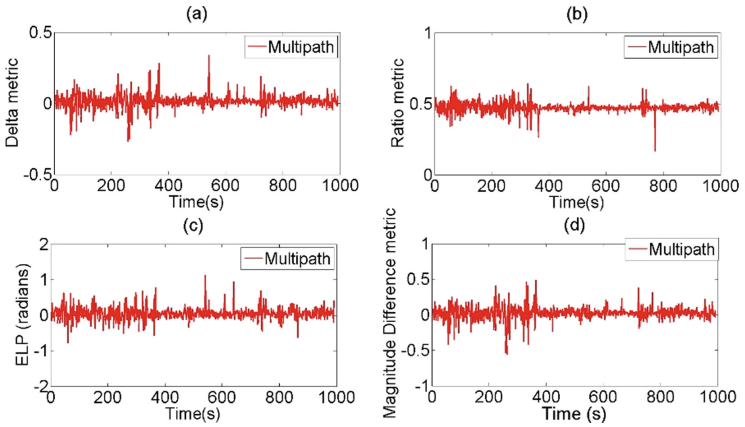

Fig. 4. The four metric responses: (a) Delta (b) Ratio (c) ELP (d) Magnitude Difference, in a multipath environment corresponding to a drive in Osaka and processed with a 0.56 chip correlator spacing.

4 Detection Process Using Moving Variance

4.1 Moving Variance Definition and Distribution

Considering the change in carrier-to-noise ratio (C/N0) during an attack, a method called moving variance monitoring variances of C/N0 is proposed to detect spoofing in the second step [12]. Moreover, multipath can easily be distinguished from deception as a result of its short duration peaks.

Through a predefined window sizing a subset of metric values, the moving variance formula evaluates the difference between the mean of the squares of the subset and the square of the mean over this subset to create a series of variances of different subsets of the full data set [12].

$$\sigma^2_{MV}(n) = \frac{1}{W}\sum_{i=(n-1)*W+1}^{n+W} x(i)^2 - \left(\frac{1}{W}\sum_{i=(n-1)*W+1}^{n+W} x(i)\right)^2 \tag{5}$$

where,

$x(i)$ is the value of the i-th sample in the data,
W the length of one subset,
n the number of subsets of size W in the data.

In order to further improve the detection performance, carrier power was additionally used for two-dimensional observation and is calculated by the given formula.

$$Pd = 10 * \log\left(\sqrt{2\left(\overline{\|R(x)\|^2}\right)^2 - \overline{\|R(x)\|^4}}\right) \tag{6}$$

and,

$$R(x) = I_p(x) + i * Q_p(x) \tag{7}$$

where, $I_p(x)$ and $Q_p(x)$ are the xth prompt correlator output of in-phase (I) and quadrature(Q) branch, respectively.

4.2 Thresholds Determination

Threshold in Time. To exclusively detect spoofing without multipath peaks, the moving variance curve needs to be evaluated in terms of its width as well as its height by a double threshold method. If the moving variance exceeds the predefined threshold during a certain amount of time defined as a threshold in time, a spoofing attack alert will then be triggered.

Threshold on Moving Variance Value. It has been studied to achieve a typical detection method for the establishment of a threshold over a set of data [13, 14] and more rigorous techniques for establishing a threshold on SQM metrics have also been studied [15].

Then, we can come to the conclusion that to get a threshold, the moving variance distribution has to be estimated with regards to a clear data (the considered signal neither affected by spoofing nor multipath). However, such estimations are not suitable with real time computation, as long as the distribution is dependent on the window size, the number of samples of correlator's outputs and the receiver's sampling frequency.

Therefore, the hypothesis was assumed that the moving variance of a clear signal without the effects of spoofing or multipath can be distributed through a Gaussian distribution and the threshold computed from this signal can then be used for the basic statistical detection method [3].

For each PRN and SQM metric, the threshold Th is computed as [3].

$$Th = m* + m_{exp} \times \sigma \tag{8}$$

where,

$m*$: The long term mean value of the clear signal moving variance,
m_{exp}: The expansion factor related to the probability of a false alarm by Table 2 under the hypothesis of a Gaussian distribution,
σ: The standard deviation of the clear signal moving variance.

Table 2. False alarm rate with regard to the expansion factor for a Gaussian distribution [14].

Expansion factor m_{exp}	1	2	3	4	5	6
Monitor threshold	1σ	2σ	3σ	4σ	5σ	6σ
False alarm rate	0.3173	0.0455	0.0027	6.35E-5	5.73E-7	1.97E-9

4.3 Algorithm Performance

Comparing Fig. 6 with Fig. 5, it can be seen that the moving variance helps gathering groups of low values in two stages when only authentic or counterfeit signals are tracked. In addition, it enlightens the values taken during the interaction phase as extra ones, which leads to a more available and observable threshold.

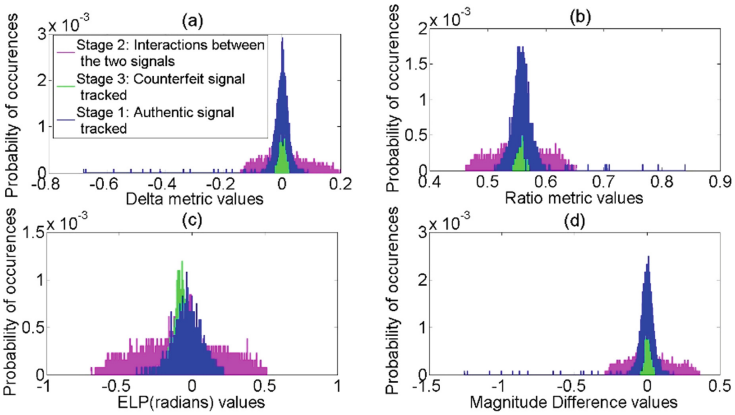

Fig. 5. Distribution of the raw metric values during the different steps of a spoofing attack in Scenario 2 from TEXBAT at 0.01 s average (a) Delta (b) Ratio (c) ELP (d) Magnitude Difference.

As shown in Fig. 7, a distinguished difference exists between the distribution in the presence of spoofing and that of the clean signal condition. The counterfeit signal has a higher power and a wider distribution of moving variance, while the authentic signal is low at both levels.

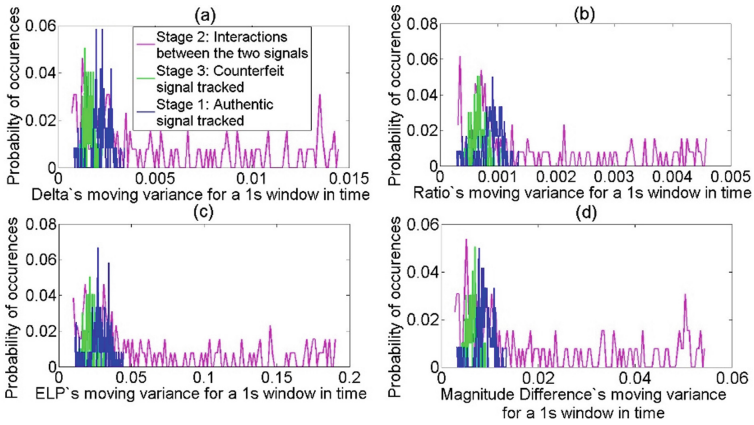

Fig. 6. Distribution of the moving variance values for a 1 s time-window during the different steps of a spoofing attack in Scenario 2 from TEXBAT (a) Delta (b) Ratio (c) ELP (d) Magnitude Difference.

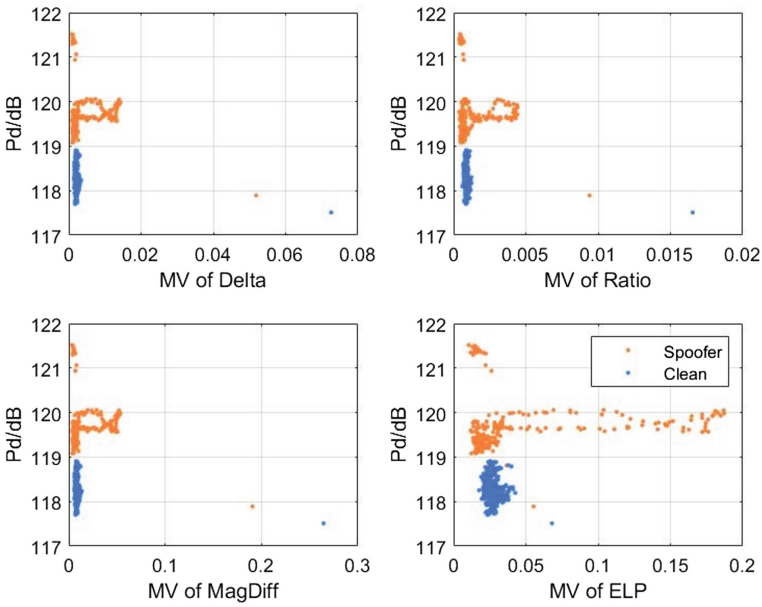

Fig. 7. Two-dimensional joint distribution of SQM metrics' moving variance for a 1 s time-window and carrier power in Scenario 2 from TEXBAT and no-spoofing scenario.

To compare the differences in the two scenarios, the gravity center of the distribution is displayed in Fig. 8 with the lines representing the distance; upper endpoints in spoofing condition and lower ones in no-spoofing. It is worth noting that the ELP metric has the longest distance, which means it is easier to establish a detection threshold. In addition, according to the formula, only the ELP value is uncorrelated with the carrier power.

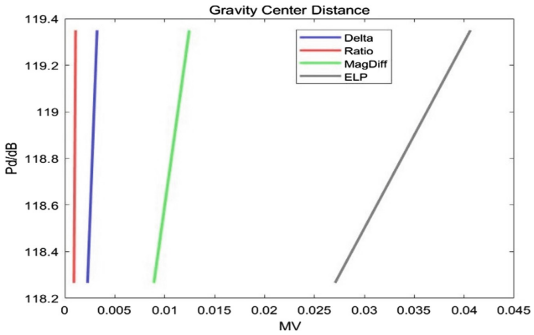

Fig. 8. Gravity center distance of two-dimensional joint distribution in Scenario 2 from TEXBAT and no-spoofing scenario.

As mentioned above, due to the short duration peaks of multipath, the moving variance values in multipath environments display a distribution as random peaks, Fig. 9, while they last for a longer time under spoofing conditions, Fig. 10.

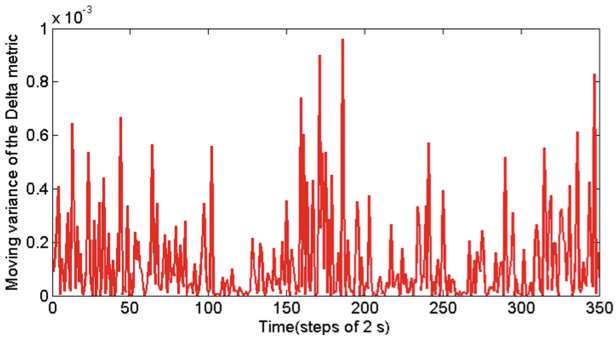

Fig. 9. Delta metric's moving variance for the signal corresponding to PRN 17 for a 0.5625 correlator spacing in a multipath environment corresponding to a drive in Osaka.

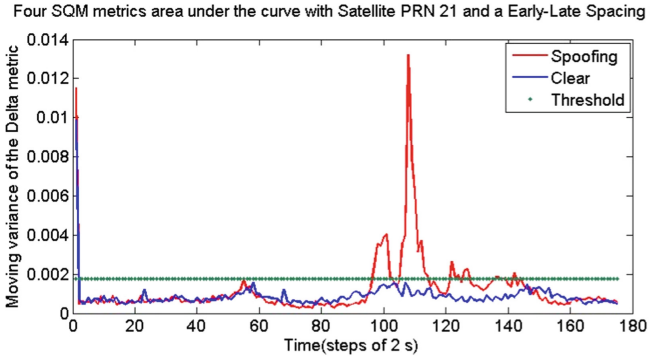

Fig. 10. Delta metric's moving variance for the signal corresponding to PRN 21 in scenario 6 from TEXBAT and its established threshold (detailed in next chapter) computed with $m_{exp} = 3$ with a 0.5 correlator spacing.

5 Conclusion

Four metrics for monitoring were adopted and their performance was compared between traditional SQM and moving variance methods. Then, a method of two-dimensional observation involving moving variance and carrier power was proposed to improve the detection performance. As a result, a distinguished difference exists between the distribution in the presence of spoofing and that of the clean signal condition, in which ELP's moving variance and the carrier power is the best combination without correlation. At last, this work verifies the feasibility of using threshold in time to distinguish spoof from multipath signals through the comparison of peak durations.

Acknowledgement. We would like to thank all those who have helped the work. First of all, we extend our sincere gratitude to the committee of Chinacom 2019 - 14th EAI International Conference on Communications and Networking in China for providing the opportunity and support. High tribute shall be paid to Joon Wayn Cheong Andrew G. Dempster and Laure Demicheli from The University of New South Wales whose profound knowledge greatly promoted this work. Finally, we are also indebted to William's team for correct language expression.

References

1. Humphreys, T.E., Bhatti, J.A., Shepard, D.P., Wesson, K.D.: The texas spoofing test batte. In: Proceedings of the ION GNSS Meeting (2012)
2. Wesson, K.D., Shepard, D.P., Bhatti, J.A., Humphreys, T.E.: An evaluation of the vestigial signal defense for civil GPS anti-spoofing. In: Proceedings of the ION GNSS Meeting (2011)
3. Demicheli L. Cetin, E., Thompson, R.J., Dempster, A.G.: Assessment of Signal Quality Monitoring (SQM) metrics performances. In: Dissertation, UNSW
4. Phelts, R.E.: Multicorrelator techniques for robust mitigation of threats to GPS signal quality. In: Doctoral dissertation, Stanford University (2001)
5. Manfredini, E.G., Dovis, F., Motella, B.: Validation of a signal quality monitoring technique over a set of spoofed scenarios. In: 2014 7th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC), pp. 1–7 (2014)
6. Jahromi, A.J., Broumandan, A., Nielsen, J., Lachapelle, G.: GPS spoofer countermeasure effectiveness based on signal strength, noise power, and C/N0 measurements. Int. J. Satell. Commun. Network. **30**, 181–191 (2012)
7. Wesson, K.D., Gross, J.N., Humphreys, T.E., Evans, B.L.: GNSS signal authentication via power and distortion monitoring. In: Draft of Article in IEEE Transactions on Aerospace and Electronic Systems, vol. X, No. X, Month 201X
8. Sun, Chao, et al.: Moving variance-based signal quality monitoring method for spoofing detection. GPS Solutions **22**(3), 1–13 (2018)
9. Cetin, E., Thompson, R.J., Dempster, A.G.: Analysis of receiver observables to spoofing attacks using software receivers. In: Seminar, UNSW
10. Broumandan, A., Jafarnia-Jahromi, A., Dehghanian, V., Nielsen, J., Lachapelle, G.: GNSS spoofing detection in handheld receivers based on signal spatial correlation. In: 2012 IEEE/ION Position Location and Navigation Symposium (PLANS), pp. 479–487 (2012)
11. Ali, K., Manfredini, E. G., Dovis, F.: Vestigial signal defense through signal quality monitoring techniques based on joint use of two metrics. In: 2014 IEEE/ION Position, Location and Navigation Symposium-PLANS 2014, pp. 1240–1247 (2014)

12. Jovanovic, A., Botteron, C., Fariné, P.A.: Multi-test detection and protection algorithm against spoofing attacks on GNSS receivers. In: 2014 IEEE/ION Position, Location and Navigation Symposium-PLANS 2014, pp. 1258–1271 (2014)
13. Tawk, Y., et al.: A new movement recognition technique for flight mode detection. Int. J. Veh. Technol. (2013)
14. Irsigler, M., Hein, G.: Development of a real time multipath monitor based on multi-correlator observations. In: Proceedings of the ION-GNSS (2005)
15. Brocard, P., Thevenon, P., Julien, O., Salos, D., Mabilleau, M.: Measurement quality assessment in urban environments using correlation function distortion metrics. In: ENAC, Egis France