Wireless Pers Commun
DOI 10.1007/s11277-017-4635-z

# A Novel Ratio-Phase Metric of Signal Quality Monitoring for Real-Time Detection of GPS Interference

**A. Farhadi[1] · M. Moazedi[1] · M. R. Mosavi[1] · A. Sadr[1]**



**Abstract** Through the growing usage of Global Positioning System (GPS) for civilian applications, healthcare of the system has special importance. However, according to the characteristics of the GPS signals, there is a possibility of interferences on GPS signals. Among all distorting factors, spoofing is more deceitful, because the civil receiver is not able to distinguish the counterfeit signal from the genuine signal. In recent years, many efforts have been made to deal with spoofing. We studied recognition of the clear certainty of a spoofed condition in this work, which focuses on Signal Quality Monitoring (SQM) method. In an effort to troubleshoot the previous metrics and methods, we have introduced a new metric for interference detection that investigate both of in-phase and quadrature components of correlation outputs also use parameters associated with the main peak in proper form. As a consequence of simultaneous evaluation of phase and amplitude of GPS signal, the proposed metric is more reliable and average of detection accuracy has increased from 1.3 (related to previous metrics) to 4.8.

**Keywords** Detection · Interference · GPS · SQM

✉ M. R. Mosavi
m_mosavi@iust.ac.ir

A. Farhadi
a_farhadi@elec.iust.ac.ir

M. Moazedi
moazedi@elec.iust.ac.ir

A. Sadr
sadr@iust.ac.ir

[1] Department of Electrical Engineering, Iran University of Science and Technology, Narmak, Tehran 16846-13114, Iran

Published online: 02 August 2017

## 1 Introduction

Dysfunction of GPS-based systems in the areas of navigation and urban applications can cause significant economic damage as well as damage to the infrastructure of the financial markets. In this regard, the Volpe report in 2001 showed the importance of spoofing threat and sought for further research in the anti-spoofing field [1]. Starting with this report, important researches in this area began and various countermeasure methods, including detection and reduction of interference effect were introduced [2–7]. GPS signal is a suitable goal to be disturbed by a spoofer because the signal received by the GPS receiver is very weak, thus a low power disruption can easily manipulate the GPS information; so that the receiver calculates the position by fault.

Generally, GPS signals can be threatened at different levels, including data processing, data structures and positioning [4–6, 8, 9]. Therefore, anti-spoofing methods must be able to perform accurately and recognize forged signals in all these sectors impressively, as well as obtaining accurate information about the correct position from the signals. Thus, the opposition process consists of two sections, detecting an attack and reducing its effect. This paper generally has focused on detecting methods. At first, we have a brief description of Signal Quality Monitoring (SQM) method. After a review of spoofing data collection which is used in our measurement, we have an evaluation of the existing SQM metrics and study strength and weakness of each one. In Sect. 5, a new enhanced metric is introduced which can be used in SQM for detecting spoofing at tracking level. In the following, there is an investigation of the suggested enhanced metric and also a comparison between the former metrics and the enhanced one.

## 2 Overview of Previous Signal Quality Monitoring Metrics to Detect Spoofing Attack

Figure 1 shows a general view of an anti-spoofing system. Up to now, several methods have been introduced to recognize counterfeit signals such as Time Of Arrival (TOA) [10], power monitoring [4–6], spatial processing [11], SQM [12–14] and Vestigial Signal Defense (VSD) [15]. In this paper, SQM has been discussed in particular. This method gets to be used for GPS correlation peak monitoring in multi-path and fade environment. SQM utilized signal monitoring and multi-path detection methods to solve the spoofing problem. Previous references [10, 12, 16, 17] have developed SQM method to detect attacks on mobile receivers which are in the line of sight. The SQM metrics can recognize abnormal sharp peaks of the signal or increment in correlation peaks and also can be used to detect any abnormal asymmetry or similarity in overhead peaks that imposes spoofing attack.

Studying and making decision for the presence or absence of an attack are usually done by using statistical hypothesis. For example, in Refs. [16, 17], SQM is implemented in code and carrier tracking level. The changes caused by the spoofing attack in tracking loop and PLL and DLL outputs can be observed. Absolute values of correlator nodes E, L and P in the specified time interval are shown in Fig. 2. As it is obvious in this figure, DLL output has non-linear changes under the influence of interference. At these moments, DLL cannot generate appropriate feedback control signal proportional to the delay between the actual Pseudo Random Noise (PRN) code and replica. As a result, synchronization is not possible in this situation and it causes destruction that can be used to recognize spoofing. A similar effect is also visible in the output of the PLL loop. Figure 3 shows the output loop PLL

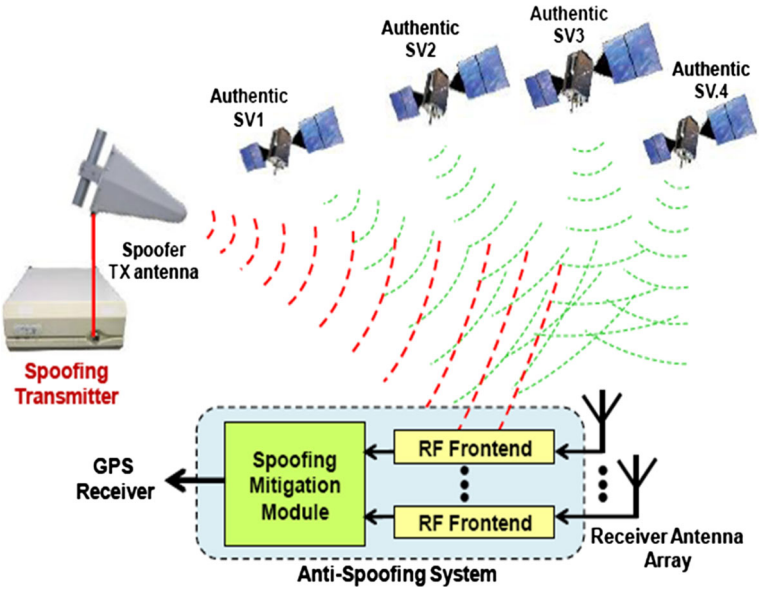



**Fig. 1** A general view of an anti-spoofing system

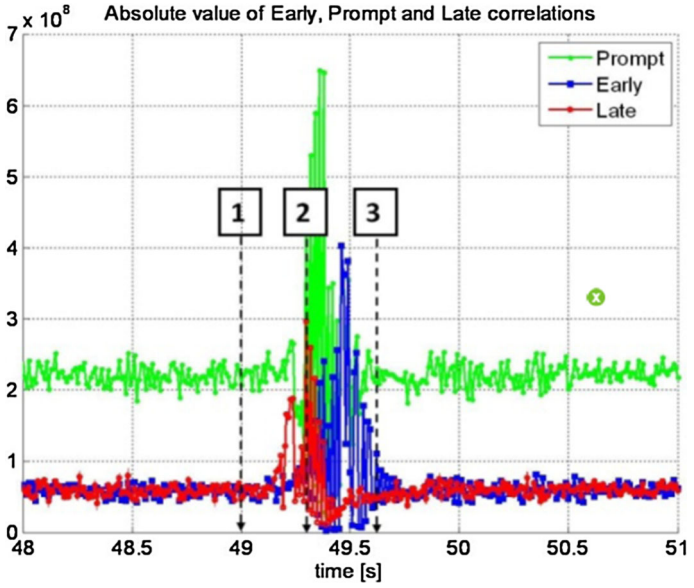



**Fig. 2** DLL loop output during the spoofing attack [16, 17]

during the spoofing attack. Despite of the fake and the same original frequency, PLL cannot provide appropriate feedback signals during the spoofing attack and has to be unlocked. After spoofing attack ended, the fake signal controls the victim receiver. Therefore, the detection algorithm must be active before the start of the spoofing attack.

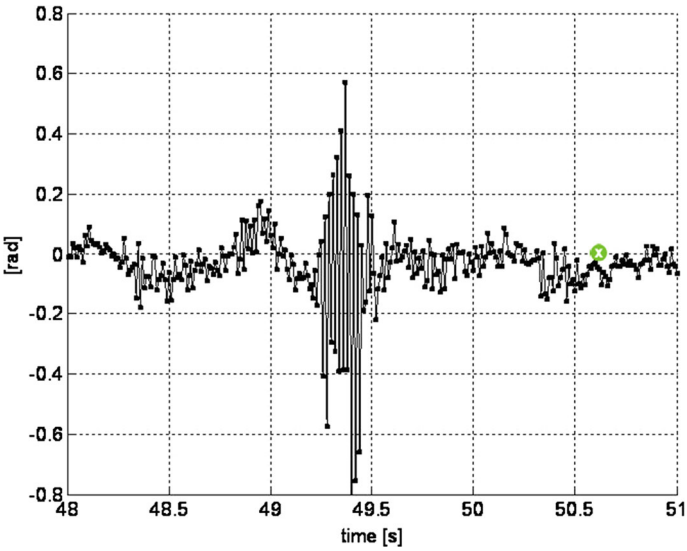



**Fig. 3** Output of the correlators E, L and P in PLL [16, 17]

Another way to detect a GPS spoofing attack is the evaluation of correlation function [4–6]. In the line of sight, that there are only the original signals and noise at the correlators output, the square amplitude of the correlator function follows the $\chi^2$ distribution with two degrees of freedom. Although, during the conflict of the original and the spoofing signal, the correlator output may not follow $\chi^2$ distribution, but the correlation peak of forgery signal must be as much as possible near the peak of valid GPS signal. Thus, the spoofing signal affects the power of the correlator and interaction between authentic and counterfeit signals causes several changes in amplitude of the correlator. These changes cause deviation from the expected $\chi^2$ distribution at the correlation output. Figure 4 compares the intermediate distribution of the correlator function in the presence and absence of fake signals with different relative powers for authentic and spoofing signals. As can be seen, through the spoofing and signal interference, output distribution of the correlators is totally different from the distribution of $\chi^2$.

The interaction between spoofing and authentic signals is similar to the interaction between multi-path and direct signals. However, differences between them causes significant challenges for any defense that is based on monitoring the complex correlation domain. One of the main discrepancies is amplitude. Multi-path signals are weaker than the genuine ones. Another discrepancy is the phase difference between the authentic and spoof signal. Multi-path signal causes a slight time delay, while the delay in a spoof signal is larger [9].

As mentioned above, SQM anti-spoofing techniques are powerful methods to detect interference. However, they may not be able to distinguish between spoofing signals and multi-path reflections. Also, if the spoofer can produce a spoofing attack without changing the maximum of signal correlation, this method cannot recognize spoofing.

To improve the performance in different conditions, several solutions based on SQM have been proposed such as VSD [15]. In this method the spoofing is often modeled in the complex correlation domain. After calculation of the input signal correlation with

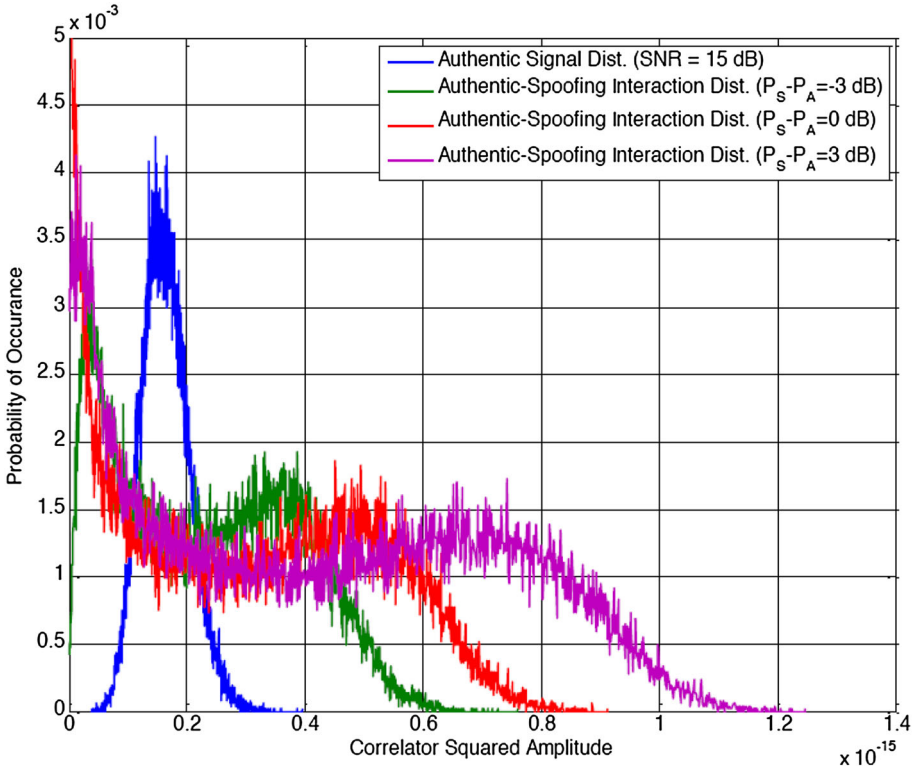



**Fig. 4** Intermediate distribution of the correlator's output in presence or absence of spoofing signals [4–6]

generated PRN, a complex correlation function of x at time t and offset delay ζ can be expressed as below:

$$x(t,\zeta) = x_d(t,\zeta) + x_m(t,\zeta) + x_s(t,\zeta) + \mathrm{n}(t,\zeta) \tag{1}$$

$x(t,\zeta)$ is a superposition of four components of the complex correlation, in which $x_d$ is direct path; indeed, it is the GPS signal. $x_m$ is multi-path component, $x_s$ are spoofing signal and n is a Gaussian white noise signal. DLL with three complex correlators (early, prompt and late) is executed in this function to trace the signal. Receivers using VSD technique generate far more correlators to increase the prediction accuracy on the degradation rate of the complex correlation function. When a series of correlator delays are available, complex correlation function can be considered as a time continuous signal. If we assume that there is no multi-path signal, spoofing signal's model $x_s(t,\zeta)$ in the complex correlation function area will be represented as:

$$x_s(t,\zeta) = (\alpha_s(\mathrm{t})\mathrm{R}(\zeta - \zeta(\mathrm{t})) \times I_{Spoofing} \tag{2}$$

If the spoofer tries to entice the victim with a fake signal that is a too close copy of the GPS signal, $x_s(t,\zeta)$ must be approximately equal to $x_d(t,\zeta)$. The only noticeable difference in this model is "$I_{Spoofing}$", that shows an attack is happening [15]. In SQM method, various metrics have been presented based on distortions in the complex correlation to detect spoofing. Actually, monitoring the destruction of the complex correlation function means

calculating a metric based on samples of the complex correlation output. In general, autocorrelation function R (ζ) model is as follows:

$$R(\zeta) \approx \begin{cases} 1 - \dfrac{|\zeta|}{\mathrm{T_C}}; & \text{for } |\zeta| < \mathrm{T_C} \\ 0; & \text{otherwise} \end{cases} \tag{3}$$

After the spoofing, $|x_s(t,\zeta)|$ does not remain as the ideal autocorrelation function $\mathrm{R}(\zeta)$. Usually the receiver uses three-point correlation point (early, prompt and late) to track the GPS signal. The destruction of the complex correlation function also can be observed in phase and square component of $x(t,\zeta)$. When there is not spoofing multi-path and noise, we have the relations $\mathrm{Q}(\mathrm{t},\zeta) = 0$ and $\mathrm{I}(\mathrm{t},\zeta) = \mathrm{R}(\zeta)$, but in the presence of spoofing, multi-path and noise, values of $\mathrm{Q}(\mathrm{t},\zeta)$ and $I(\mathrm{t},\zeta)$ changes [18]. In the following, we will briefly introduce metrics that assay changes in the correlation function [15]. The discussed metrics can help a GPS receiver to distinguish authentic signals from those forged by using a signal simulator.

## 2.1 Delta Metric

Delta metric is defined as the following equation [10]

$$\Delta_\zeta(t) = \frac{I_{E,\zeta}(t) - I_{L,\zeta}(t)}{2I_P(t)}. \tag{4}$$

Here, $I_E$, and $I_L$ are ζ seconds ahead or behind $I_\mathrm{P}$ in the phase component in time t. As it is clear in the equation, delta metric is symmetric. As a consequence, Eq. (4) can be considered as spoofing detection metric. Nonetheless, some kinds of synchronous attacks can generate forgery signals with no obvious distortion at I (t,τ) and spoofing only deforms Q (t,τ). Since this metric doesn't include quadrature component, distinguishing this kind of attacks will be impossible by delta test.

## 2.2 Ratio Metric

Ratio metric is relatively similar to delta metric, except that instead of subtracting in numerator, summation is used. This metric is defined as follows [10, 16, 19],

$$RT_\zeta = \frac{\mathrm{I_{E,\zeta}(t)} + \mathrm{I_{L,\zeta}(t)}}{2\mathrm{I_P(t)}}. \tag{5}$$

In fact, Ratio Metric and Delta Metric were originally designed to detect deformations in the C/A codes broadcast by the satellites but are also potentially useful for detecting spoofing. As can be seen in Eq. (5), change of ratio test depends on the relative difference of early-late taps with the prompt tap. However, in most cases, early and late taps are changed almost equally, but in the opposite direction.

## 2.3 Early-Late Phase Metric

This metric is the only one that considers quadrature component Q(t, ζ) calculations. Early-Late Phase is a recently proposed metric and is expressed as [18]

$$ELP_{\tau} = tan^{-1}\left(\frac{Q_{L,\tau}(t)}{I_{L,\tau}(t)} - \frac{Q_{E,\zeta}(t)}{I_{E,\zeta}(t)}\right). \tag{6}$$

Here $Q_{(E,\ \zeta)}(t)$ and $Q_{(L,\ \zeta)}(t)$ refer to $\zeta$ seconds ahead and behind prompt tap of quadrature component at time t, respectively. $ELP_{\tau}$ calculates the phase difference between initial and final correlation taps. In contrary to delta and ratio metrics, this metric has no estimation of the relative difference between prompt and side tabs. Moreover, it is unable to discern unbalancing of early and late taps.

## 2.4 Magnitude Difference Metric

This is another VSD metric to detect spoofing [15].

$$MD_{\zeta} = \frac{\left|x_{E,\zeta}(t)\right| - \left|x_{L,\zeta}(t)\right|}{\left|x_{P}(t)\right|}. \tag{7}$$

Here, $\left|x_{E,\zeta}(t)\right|$, $\left|x_{L,\zeta}(t)\right|$ and $\left|x_{P}(t)\right|$ are the absolute value of the correlation function for the initial value $x_{E,\zeta}(t)$ and the final value $x_{L,\zeta}(t)$ and $x_{P}(t)$, respectively. This metric is similar to delta metric. The difference is that the absolute value of the correlations is used. With regard to the fact that this metric puts the magnitude of correlation function to use, variations of in-phase and quadrature components may partly negate each other. Therefore, it is expected that this metric has low sensitivity to spoofing.

## 2.5 Ratio Test Metric

This measure is also intended in some references to recognize spoofing and is calculated as follows:

$$R_{\delta} = \frac{I_{E\zeta_i^{\frac{\delta}{2}}} + I_{L,\zeta_i^{\frac{\delta}{2}}}}{\alpha P_i} \tag{8}$$

where $\delta$ is the correlator spacing between $I_{E,\tau}(t)$ and $I_{L,\tau}(t)$ and $\alpha$ is the correlation main peak slope [16, 17]. By adjusting $\delta$ and $\alpha$, sensitivity and accuracy of metric can be enhanced. However, the mentioned problems for ratio metric are extant here.

## 2.6 Other Metrics

Other metrics usually use binary delta differencing $(\Delta_{T2}(t) - \Delta_{T1}(t))$ or simple ratios such as $I_{E,\zeta}(t)/I_{L},\zeta(t)$ [15].

Afterwards, the evaluation of just explained metrics and their effectiveness will be discussed, and to solve potential problems of existing metrics, a new one will be introduced. Before that, in order to understand the results better, we will briefly explain how to generate the utilized delay spoofing data set.

## 3 Data Collection

Saving and delaying the authentic signal is earlier investigated [20] and this scenario is known as relay deception. Pragmatic examples of receiver-spoofer are built by adding spoofer software with spreading circuit to the typical GPS receiver [8]. Practical implementation of a delayed spoofing scenario, demands equipment that can store the received RF signal in GPS receiver antenna. After applying required pre-processing with high speed to the signal, the new counterfeit signal is returned to RF field and re-sent to the target receiver. Thus, the IF signal's quantization error does not cause a problem in generating spoofing signal. Due to the lack of facilities, GPS signal simulator is used to povide the fake signal. Overview of the accomplished system in practice can be observed in Fig. 5. The corrupted signal in this attack can be expressed in Eq. (9):

$$d(n) = S(n) + \alpha\hat{S}(n-\tau) \tag{9}$$

where "α" is amplification factor and equals to 2 here. According to the above-mentioned modeling, the delayed signal "$\alpha\widehat{S}(n-\tau)$" is actually considered as interference element emerged from a simulator. In this scenario, it is generally assumed that simulator's output is much the same signal directly taken from the GPS antenna. By changing the data runtime, spoofing data in various scales were provided. The delays in various scenarios are 4, 6 and 8 s. Different levels of spoofing error were classified into three groups with low, medium and high spoofing. Table 1 lists some examples of each group and specifies the position error in East,

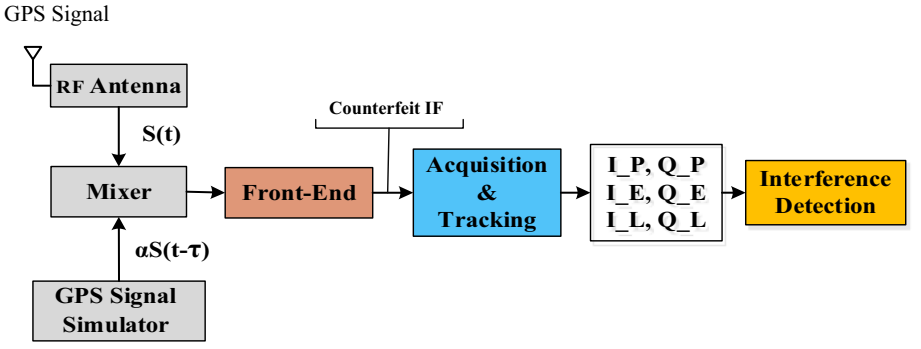



**Fig. 5** Mechanism of implanted system in practice

**Table 1** Details of some example spoofing signals

| Spoofing range | Delay time (s) | $\Delta U$ (m) | $\Delta N$ (m) | $\Delta E$ (m) | $RMS$ (m) |
|---|---|---|---|---|---|
| Low spoofing error | 4 | 73 | 9 | 109 | 81 |
| | 6 | 47 | 16 | 114 | 103 |
| | 8 | 48 | 28 | 118 | 104 |
| Middle spoofing error | 4 | 112 | 26 | 144 | 87 |
| | 6 | 103 | 16 | 195 | 166 |
| | 8 | 125 | 18 | 236 | 199 |
| High spoofing error | 4 | 310 | 59 | 412 | 265 |
| | 6 | 266 | 324 | 484 | 242 |
| | 8 | 204 | 314 | 535 | 382 |

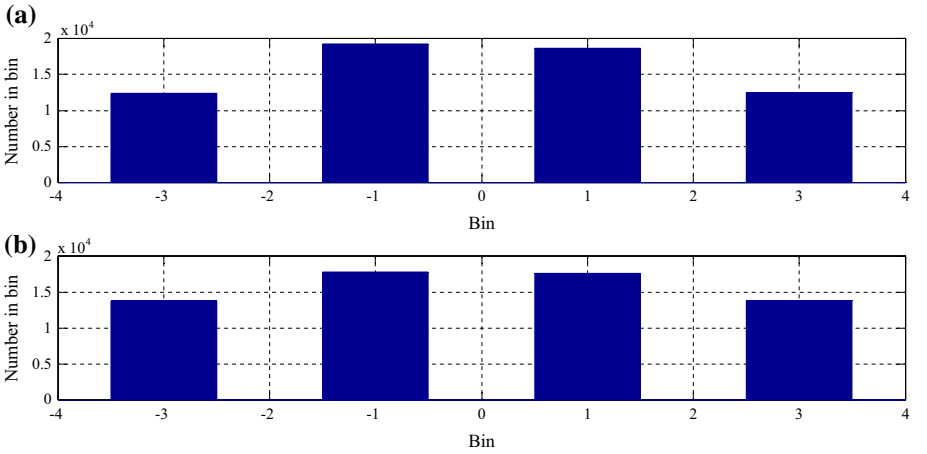



**Fig. 6** Histogram: **a** authentic signal and **b** spoofing signal

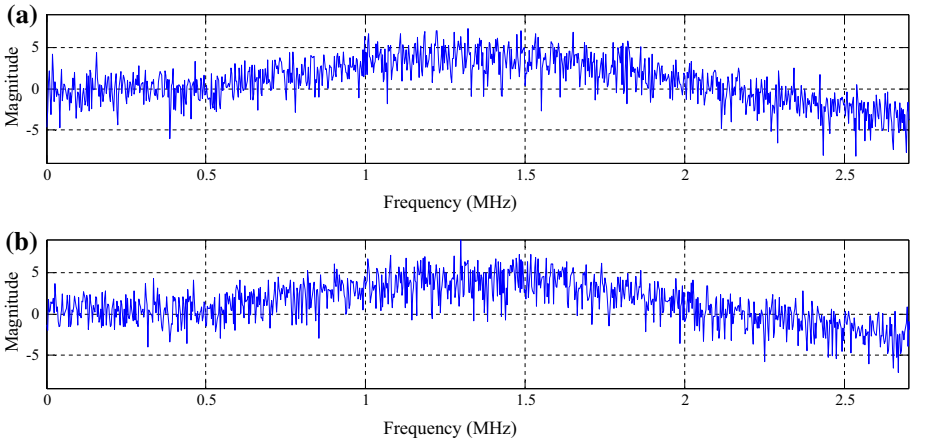



**Fig. 7** Power density: **a** authentic signal and **b** spoofing signal

North and Up (ENU) coordinates. RMS refer to the position's difference between navigational solutions based on authentic and spoof signals, $\Delta H$ is height difference and $\Delta E$ and $\Delta N$are variation in surface horizons. Histogram, frequency domain and acquisition output for one of them are shown in Figs. 6, 7 and 8, respectively. As can be seen, there is no obvious difference between features of two signals. Moreover, statistical distribution and frequency domain of the two signals are similar. The counterfeit signal contains four satellites of authentic signal and prevents the other two satellites to pass the tracking segment.

## 4 Evaluation of Metrics and Their Effectiveness to Detect Spoofing

In this study, we used the measured data to evaluate the performance of the existing SQM metrics. In this data set, delay spoofing attacks in three time intervals (4, 6 and 8 s) have been implemented. To evaluate these metrics, we have executed them in software GPS

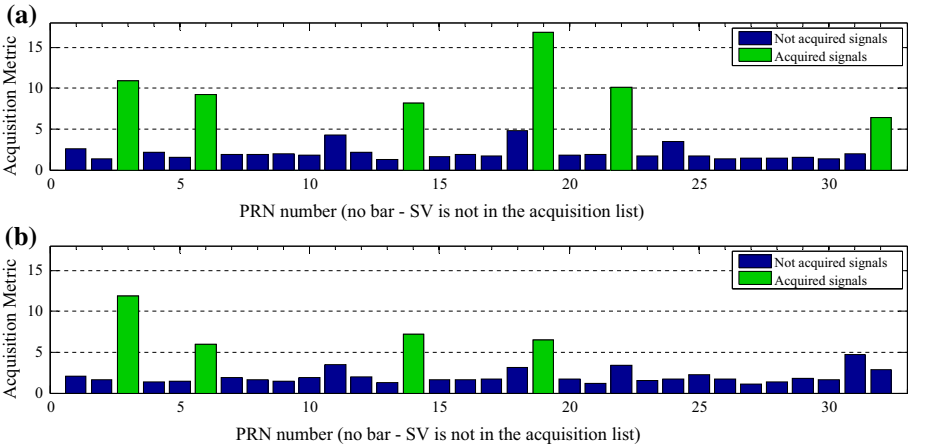



**Fig. 8** Acquisition result: **a** authentic signal and **b** spoofing signal

receiver and then investigated metric variations during the attack. For a more scientific and precise evaluation, we have defined an accuracy scale in the Eq. (10) and compare the metrics by using this scale.

$$\text{Accuracy scale} = \frac{\text{RMS of the metric after the spoofing attack}}{\text{RMS of the metric before the spoofing attack}} \tag{10}$$

The amplitudes of the metrics before applying spoofing are reported in the first column of Table 2. We also measured accuracy of all the metrics for all the 44 spoofing data that were accessible. It is obvious that the higher accuracy scale causes the easier detection and probability of false alarm can be reduced. For each of the metrics, third column of Table 2 reports the average accuracy scale for the all the data series. Success or failure in detection of an attack can be determined by evaluating accuracy factor and also the observation of the signal amplitude before and after spoofing. An important issue is threshold determination. Obviously it will be different for various metrics. Moreover, signal characteristics such as power variations in different positions. Therefore, each metric threshold cannot be completely fixed. To solve this problem threshold of each metric will be 20% higher than its value in normal mode. In this way, we can conclude that threshold accuracy factor of a successful detection is 1.2 and accuracy rate below that shows an unsuccessful detection.

In Fig. 9, by applying spoofing data we have analyzed delta metric. In this figure, the horizontal axis represents time in seconds and the vertical axis shows the amount of delta

**Table 2** Amplitude range before spoofing and accuracy factor of SQM metrics

| SQM metric | Amplitude range | Accuracy factor | RMS before attack | RMS after attack |
|---|---|---|---|---|
| Delta | −0.5, +0.5 | 1.54 | 0.16 | 0.21 |
| Ratio | 0.3, +0.8 | 1.20 | 0.53 | 0.64 |
| Early-late phase | −1.5, +1.5 | 1.39 | 0.43 | 0.54 |
| Magnitude | −0.5, +0.5 | 1.42 | 0.11 | 0.14 |
| Ratio test metric | 0, 0.1 | 1.27 | 0.05 | 0.07 |

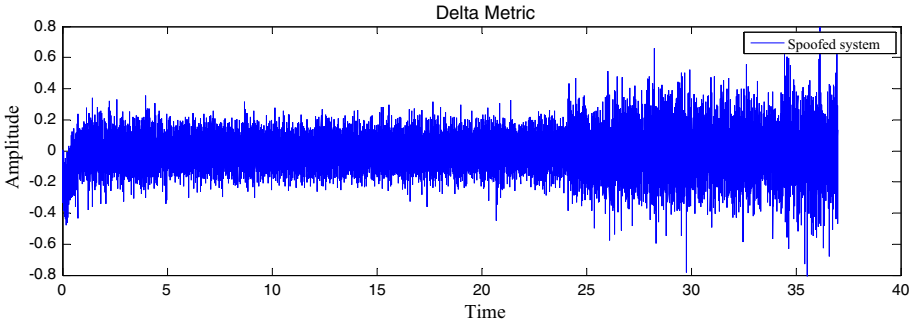



**Fig. 9** Delta metric's variation caused by applying spoofing

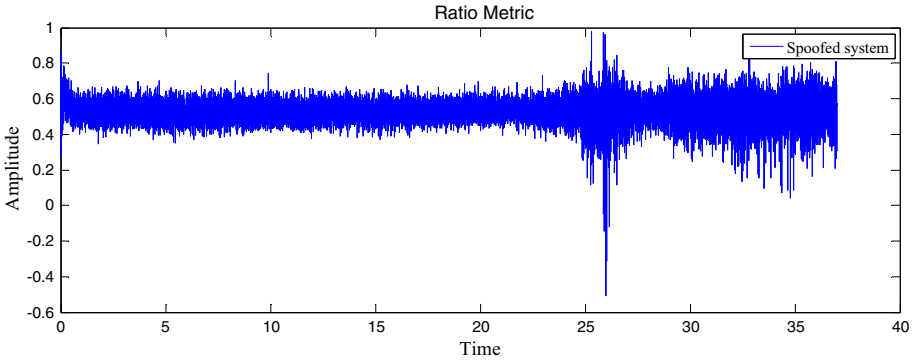



**Fig. 10** Ratio metric's variation caused by applying spoofing

metric per second. As it can be observed, at first, the metric changes in the range [−0.2, +0.2], after applying spoofing in second 24 the variation range increases to range [−0.5, +0.5] approximately. The accuracy factor in this simulation is 1.6. This situation reflects the incidence of spoofing attack and also shows that delta metric is capable to identify a satellite signal as being spoofed. In Figs. 10 through 13 the effect of spoofing attack on other metrics has been studied, respectively. Figure 10 demonstrates ratio metric variations. As can be seen, this metric's bound increases from range [0.4, 0.6] to [0.2, 0.8] after applying the spoofing attack and accuracy factor is 1.005. It illustrates successful spoofing detection of the ratio metric.

Figure 11 shows early-late phase metric. This metric is also increasing from range [−0.5, +1] to [−1.5, +1.5] which is a significant deviation. The accuracy factor (1.51) and the amplitude variation illustrates that spoofing is determined by this metric too. Similarly, in Fig. 12, applying spoofing attack brings about a considerable change in the amount of magnitude metric. In this way, the range of this metric after attack changes from range [−0.2, 0.2] to [−0.4, 0.4] with an accuracy factor of 1.57 and spoofing is determined by this metric, correspondingly. Finally, Fig. 13, which measures ratio test metric, denoting a small deviation in range [0, 0.05] affected by spoofing attack in which the accuracy factor is 1.03.

As we show through the examples, significant deviation in the amplitude of all the metrics is the result of spoofing attack which means that all of them have been capable of

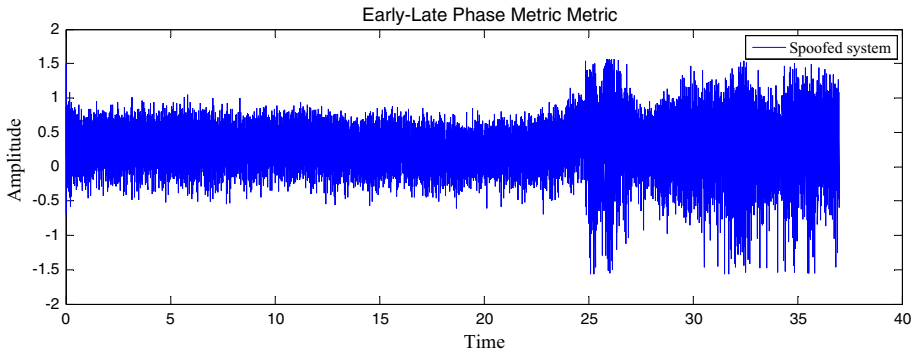



**Fig. 11** Early-late phase metric's variation caused by applying spoofing

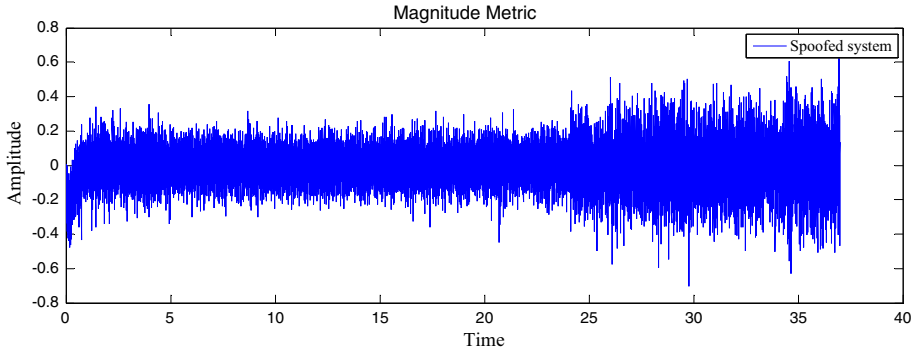



**Fig. 12** Magnitude metric's variation caused by applying spoofing

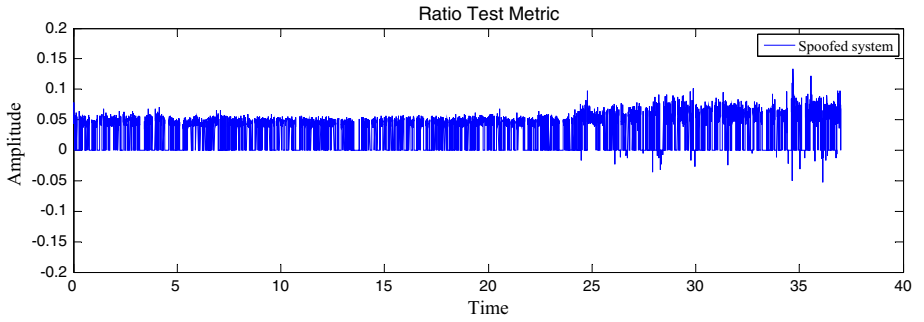



**Fig. 13** Ratio test metric's variation caused by applying spoofing

detecting the attack in specified interference data in our laboratory. However, by more examining, it was observed that it is not generally true for all spoofing data set. For instance, Fig. 14 shows that delta metric is not capable to identify spoofing attack in the data with a 6 s delay and 256 position error. As can be seen in this figure, the amplitude of this metric has not been changed significantly as a consequence of the attack and the accuracy factor of 0.77 also proves this failure. In Fig. 15, the failure of detecting spoofing

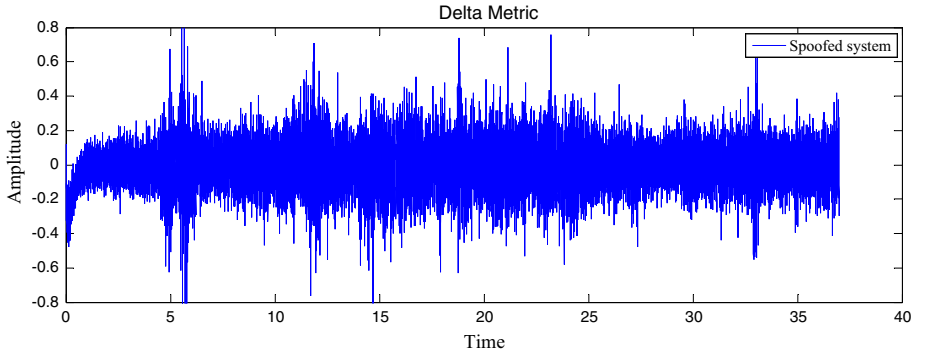



**Fig. 14** An example of failure in spoofing attack recognition by delta metric

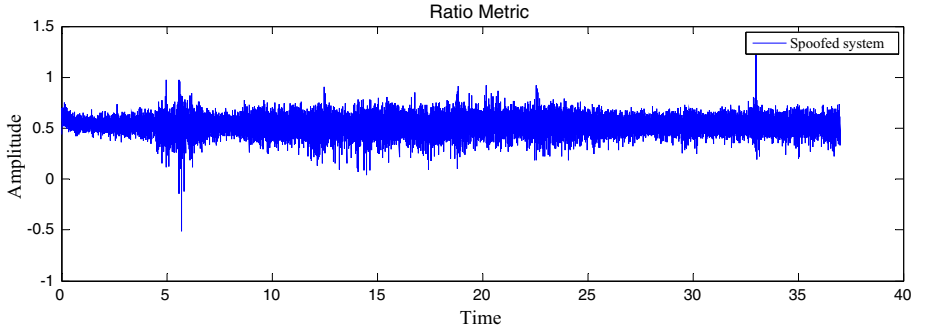



**Fig. 15** An example of failure in spoofing attack recognition by ratio metric

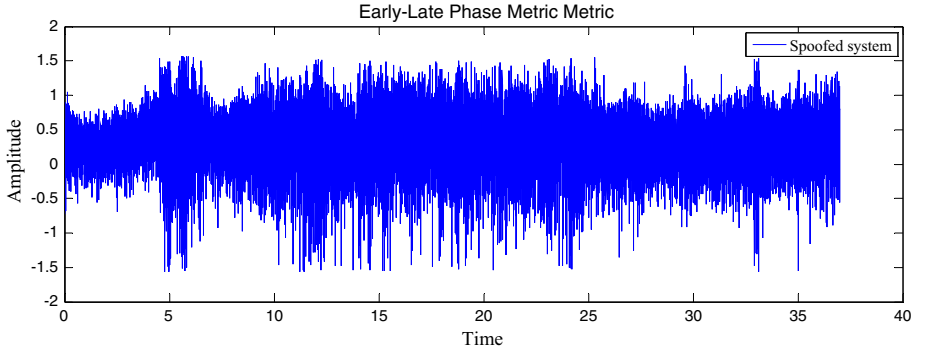



**Fig. 16** An example of failure in spoofing attack recognition by early-late phase metric

by the ratio metric is depicted for the same data as the previous figure with an accuracy factor of 1. Figures 16, 17 and 18, show the inefficiency of early-late phase metric (accuracy factor 0.84), magnitude (accuracy factor 0.86) and ratio test metric (accuracy factor 0.91) respectively for different data series. As a deduction from these examples, not all the available spoofing signals can be detected by all the existing metrics.

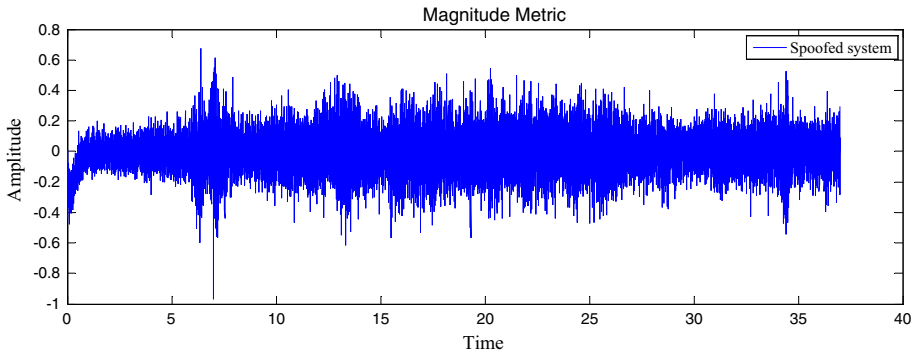



**Fig. 17** An example of failure in spoofing attack recognition by magnitude metric

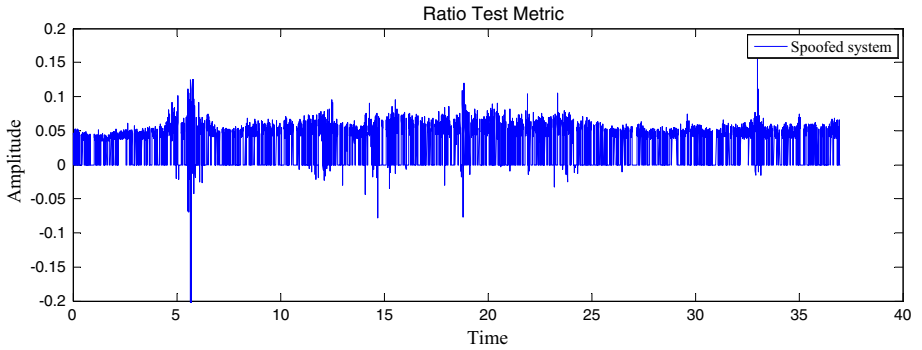



**Fig. 18** An example of failure in spoofing attack recognition by ratio test metric

## 5 Proposing the New Enhanced SQM Metric

As mentioned earlier, listed ratios in previous section belong to a data set that the relevant metrics discern them successfully. It is worse to note that outliers are excluded from the computations. Table 3 shows counterfeit datasets that have not been discerned by existing metrics. In this table, failure of interference detection is indicated by "0" and successfully detecting the attack by the metric is shown by "1". According to the simulation results, there is not any metric capable to detect spoofing attack in all specific data series. For instance, ratio metric is not able to recognize spoofing attack in data with 6 s delay and 259 meters spoofing error, while other metrics are successful in detection. For some data, only one metric is capable to identify the spoofing. As an example, the only metric which is able to detect the counterfeit data with 6 s delay and 59 meters position error is early-late phase metric. The main result obtained from investigating Table 3 is that none of the existing metrics can identify the interference correctly in all data series.

Moreover, according to the Table 2, detection accuracy for some of these metrics is very low. As a consequence, the GPS system will not meet the requirement for high security by using these metrics. Hence, the necessity for introducing a new metric which not only detect spoofing correctly in all data set, but also reveal the spoofing with higher accuracy (in other words a new metric which has a higher RMS) is clearly observable. The

**Table 3** Comparison among different metrics and their effectiveness against different data sets

| Data set | | Metrics | | | | |
|---|---|---|---|---|---|---|
| Delay (s) | Spoof error (m) | Early-late phase | Delta | Magnitude | Ratio | Ratio test |
| 4 | 109 | 1 | 1 | 1 | 0 | 0 |
| | 104 | 1 | 1 | 1 | 1 | 0 |
| | 102 | 1 | 0 | 0 | 0 | 0 |
| 6 | 256 | 1 | 0 | 0 | 0 | 0 |
| | 259 | 1 | 1 | 1 | 0 | 1 |
| | 200 | 1 | 0 | 0 | 1 | 1 |
| | 243 | 1 | 1 | 0 | 0 | 1 |
| 8 | 237 | 0 | 1 | 1 | 0 | 1 |
| | 124 | 1 | 0 | 0 | 0 | 0 |

combination of two or more existing metrics can help us to achieve a new metric which has less weakness in comparison with the old ones to get the desired result.

By studying previous metrics, we concluded that the community of early-late phase metric and delta metric is able to correctly analyze and detect the spoofing in all data set. To achieve the new metric, we review this two metrics's equations. As it can be obtained from Eq. (6) this is the only metric that considers quadrature component Q(t,τ) in the calculation. It is the main advantage of this metric rather than others, and its effects are explicit in Tables 2 and 3. As it can be seen in these tables, early-late phase metric has better performance than other metrics. On the other hand, another difference that can be perceived by comparing the delta and phase metrics is the lack of using parameters associated with the main peak (Ip and Qp) in the calculation of the phase metric. Thus, it can be deduced that the proposed metric should consider the quadrature component and also use parameters associated with the main peak in its equation so a better comparison can be done. For this purpose, the relative phase metric as a new SQM metric is proposed in Eq. (11):

$$\mathrm{RFM} = \arctan\left(\frac{\frac{Q_{L,\zeta}(t)}{I_{L,\zeta}(t)} - \frac{Q_{E,\zeta}(t)}{I_{E,\zeta}(t)}}{\frac{Q_P(t)}{I_P(t)}}\right) \tag{11}$$

## 6 Evaluation of the Proposed Metric and Comparison with Previous Ones

After executing simulations by MATLAB software on available data set, it was observed that the proposed metric works better than other metrics in terms of efficiency and accuracy. The effectiveness of this measure is shown in Fig. 19. The main feature of this metric is the minimum range before applying the spoofing and also considerable amplitude variations after the attack. This feature is predictable, according to the predefined metric relation which we called relative phase metric. In this metric's equation, unlike others (except phase metric) the quadrature component is considered and as a consequence the proposed metric has higher sensitivity in comparison with the pervious metrics. Contrary to the early-late phase SQM test, it also takes the main peak related parameters into account. This causes the low range of the metric before applying the trick and the relatively high

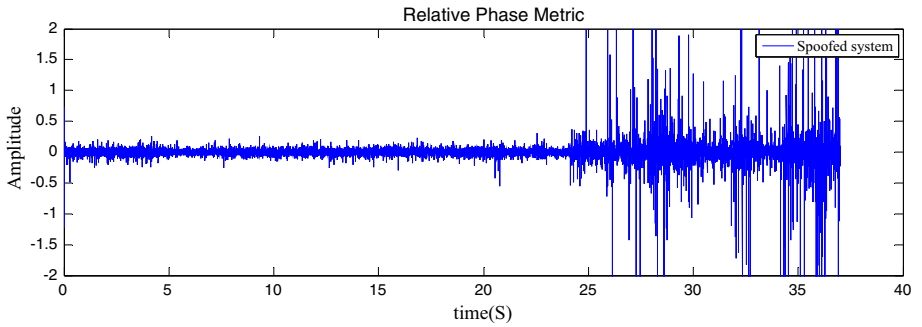



**Fig. 19** Changes of the relative phase metric affected by spoofing attack

amplitude after that. This difference will increase the accuracy of the metric. The simulations also illustrate that the proposed metric is sensitive to the spoofing in all data set and is capable to recognize interference in all of them. The relative phase metric's accuracy is significantly improved in comparison with other metrics. According to the simulations the accuracy rate has been improved from an average rate of 1.38–4.8 which leads to the issue that this SQM test is much more efficient than other SQM metrics. In other word, previous metrics are not able to distinguish between un-spoofed and spoofed signals as reliably as the suggested one.

Figures 20, 21, 22, 23, 24 show some examples of spoofing attack detection by proposed metric which have not been detected by other metrics previously. In this set of

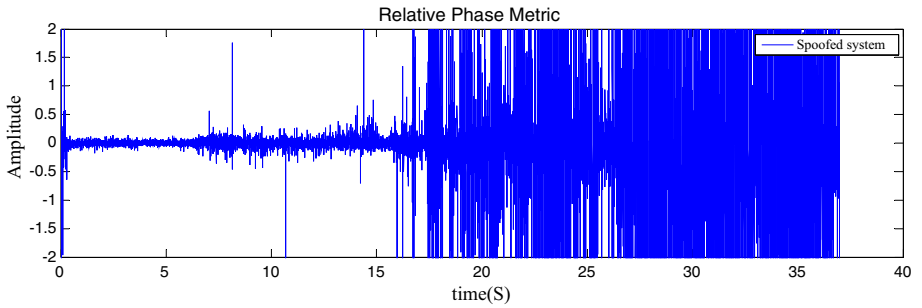



**Fig. 20** Spoofing attack detection by proposed metric which have not been detected by delta metric

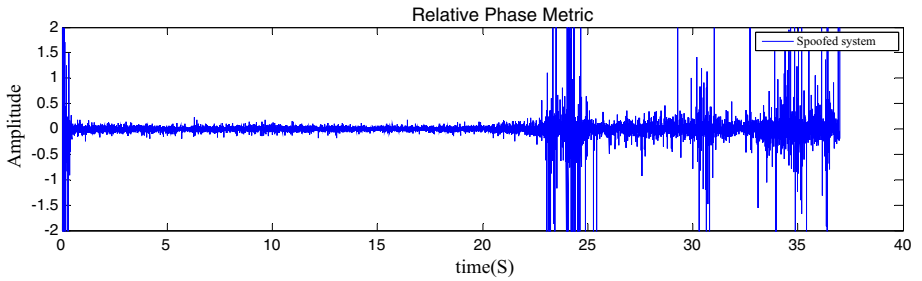



**Fig. 21** Spoofing attack detection by proposed metric which have not been detected by ratio metric

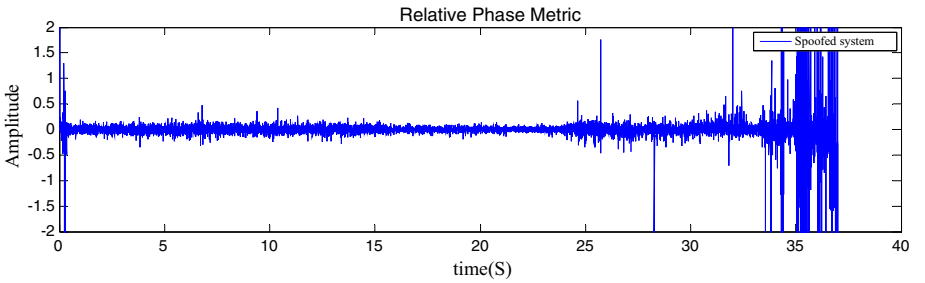



**Fig. 22** Spoofing attack detection by proposed metric which have not been detected by early-late phase metric

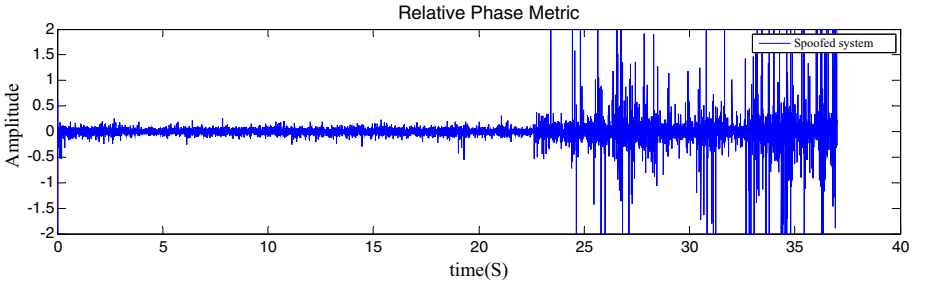



**Fig. 23** Spoofing attack detection by proposed metric which have not been detected by magnitude metric

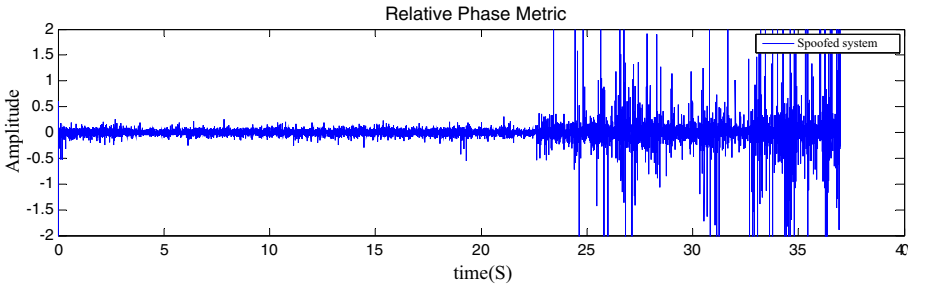



**Fig. 24** Spoofing attack detection by proposed metric which have not been detected by ratio test metric

figures, a same spoofing data is applied to the software as was given for the simulation of Figs. 14, 15, 16, 17, 18.

## 7 Conclusion

Growing importance and GPS applications in various fields, leads many researches to the security of GPS systems and investigation of eventual perturbations in them. In this study, we focused on spoofing threat as an important disturbance and analysis SQM methods as a considerable spoofing detection method in tracking level. After introducing SQM technique, conventional SQM metrics were described and then this metrics were examined by

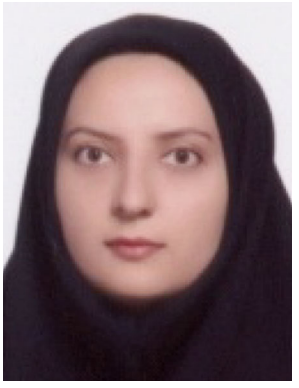
available spoofing data series in laboratory. To achieve a more precise investigation, we defined an accuracy scale and compared the conventional metrics with the defined scale. After examination of the metrics, it was concluded that none of the existing metric is capable to diagnose spoofing attack in all available spoofing data set, and furthermore, in some cases they do not have sufficient accuracy. As a consequence, the immense necessity for a new metric is undoubted. By the combination of the conventional metrics a novel enhanced metric has been obtained. By the evaluation of the new ratio phase metric and comparing it with the other tests, it was concluded that the proposed enhanced metric has improved considerably in terms of efficiently and accuracy in spoofing real-time detection. Base on this paper, because of simultaneous consideration of phase and amplitude of GPS signal in the suggested metric, detection accuracy increases from average 1.3 (related to previous metrics) to average 4.8 which is which is an impressive improvement.

## References

1. Volpe, J. A. (2001). Vulnerability assessment of the transportation infrastructure relying on global positioning system. *National Transportation Systems Center, Technical Report.*
2. Baziar, A. R., Moazedi, M., & Mosavi, M. R. (2015). A wavelet based spoofing error compensation technique for Single frequency GPS stationary receiver. In *The 1st National Navigation Conference, Sharif University of Technology*, pp. 1–6.
3. Baziar, A. R., Moazedi, M., Mosavi, M. R., & Ghaffari, Z. (2014). A new method for GPS spoofing detection based on pseudo-range measurement in naval applications. *Journal of Marine Science University of Imam Khomeini, 2*(1), 8–21.
4. Jahromi, A. J., Broumandan, A., Nielsen, J., & Lachapelle, G. (2012). GPS vulnerability to spoofing threats and a review of anti-spoofing techniques. *International Journal of Navigation and Observation, 2012,* 1–16.
5. Jahromi, A. J., Broumandan, A., Nielsen, J., & Lachapelle, G. (2012). GPS spoofer countermeasure effectiveness based on signal strength, noise power, and C/N0 measurements. *International Journal of Satellite Communications and Networking, 30*(4), 181–191.
6. Jahromi, A. J., Lin, T., Broumandan, A., Nielsen, J., & Lachapelle, G. (2012). Detection and mitigation of spoofing attacks on a vector-based tracking GPS receiver. In *International Technical Meeting of the Institute of Navigation* (*ION ITM*), pp. 3–8.
7. Mosavi, M. R., Rezaei, M. J., Hosseinzadeh, N., & Kiaamiri, R. A. (2014). New intelligent methods for detection and mitigation of spoofing signal in GPS receivers. *Journal of Electronics and Cyber Defense, 2*(1), 71–81.
8. Baziar, A. R., Moazedi, M., & Mosavi, M. R. (2015). Analysis of single frequency GPS receiver under delay and combining spoofing algorithm. *Wireless Personal Communications, 83*(3), 1955–1970.
9. Shepard, D. P., & Humphreys, T. E. (2010). Characterization of receiver response to spoofing attacks. *GPS World, 21,* 27–33.
10. Ledvina, B. M., Bencze, W. J., Galusha, B., & Miller, I. (2010). An In-line anti-spoofing module for legacy civil GPS receivers. In *Proceedings of the ION ITM, San Diego, CA.*
11. Montgomery, P. Y., Humphreys, T. E., & Ledvina, B. M. (2009). A multi-antenna defense: Receiver-autonomous GPS spoofing detection. *Inside GNSS, 4*(2), 40–46.
12. Mitelman, A. M. (2004). Signal quality monitoring for GPS augmentation systems (Doctoral dissertation, Stanford University).
13. Phelts, R. E. (2001). Multi-correlator techniques for robust mitigation of threats to GPS signal quality (Doctoral dissertation, Stanford University).
14. Pini, M., Fantino, M., Cavaleri, A., Ugazio, S., & Presti, L. L. (2001). Signal quality monitoring applied to spoofing detection. In *The 24th International Technical Meeting of the Satellite Division of the Institute of Navigation* (*ION GNSS*), pp. 1888–1896.
15. Wesson, K. D., Shepard, D. P., Bhatti, J. A., & Humphreys, T. E. (2011). An evaluation of the vestigial signal defense for civil GPS anti-spoofing. In *The 24th International Technical Meeting of the Satellite Division of the Institute of Navigation* (*ION GNSS*), pp. 1–11.

16. Cavaleri, A., Motella, B., Pini, M., & Fantino, M. (2010). Detection of spoofed GPS signals at code and carrier tracking level. In *IEEE Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC)*, pp. 1–6.
17. Cavaleri, A., Motella, B., Pini, M., & Fantino, M. (2010). Detection of spoofed GPS signals at code and carrier tracking level. In *5th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing*.
18. Mubarak, O. M., & Dempster, A. G. (2010). Analysis of early late phase in single-and dual-frequency GPS receivers for multipath detection. *GPS Solutions, 14*(4), 381–388.
19. Cavaleri, A., Pini, M., Presti, L. L., Fantino, M., Boella, M., & Ugazio, S. (2011). Signal quality monitoring applied to spoofing detection. In *Proceedings of the ION GNSS Meeting, Portland, OR.*
20. Tippenhauer, N. O., Pöpper, C., Rasmussen, K. B., & Capkun, S. (2011). On the requirements for successful GPS spoofing attacks. In *The 18th ACM conference on Computer and Communications Security*, pp. 75–86.

**A. Farhadi** received her B.S. degrees in Electronic Engineering from Iran University of Science and Technology (IUST), Tehran, Iran in 2015. Her research interests in the area of digital electronics, field-programmable gate array and VLSI systems.



**M. Moazedi** received her B.S. and M.S. degrees in Electronic Engineering from IUST, Tehran, Iran in 2008 and 2011, respectively. She is currently Ph.D. student of IUST Department of Electrical Engineering. Her research interests in the area of analog and mixed signal integrated circuits, GPS security and integrity.

**Mohammad-Reza Mosavi** received his B.S., M.S., and Ph.D. degrees in Electronic Engineering from Iran University of Science and Technology (IUST), Tehran, Iran in 1997, 1998, and 2004, respectively. He is currently faculty member (full professor) of the Department of Electrical Engineering of IUST. He is the author of more than 300 scientific publications in journals and international conferences. His research interests include circuits and systems design.

**Ali Sadr** received his B.S. degree in Electronic Engineering from AmirKabir University of Technology, M.S. from IUST and Ph.D. from University of Manchester Institute of Science & Technology in 1988, 1992 and 2002, respectively. He is currently faculty member of Department of Electrical Engineering of IUST as an associate professor. His research interests include non-destructive evaluation, digital systems and signal processing.