Int. J. Nonlinear Anal. Appl. 16 (2025) 1, 147–161
ISSN: 2008-6822 (electronic)
http://dx.doi.org/10.22075/ijnaa.2024.32691.4866

Anti-spoofing by smart acquisition in cold-start with multiple hypothesis using wavelet transform in a software GPS receiver

Maryam Moazedi[a,*], Mohammad Reza Mosavi[b]

[a]Department of Engineering Sciences, Advanced Technologies, University of Mohaghegh Ardabili, Namin, Iran

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

(Communicated by Haydar Akca)

Abstract

The spoofing subject is becoming ever increasingly more severe. In addition to the flow of technology, the availability of software-defined radio platforms has increased. Usually, detecting the spoofing is performed by introducing the features that are difficult for the deceiver to counterfeit. Spoofing and countering can be performed in different parts of a GPS receiver. In recent years, less attention has been paid to defense at cold-start. This research presents that the spoofing attack can be diminished during the initial start-up process with a very short effective time. This low-cost method introduces a new decision rule based on a multiple statistical hypothesis test to identify fake peaks in correlation output of acquisition and extract the authentic peaks utilizing the wavelet transform or peak removal process. The main distinction of this method with previous works is investigating different amplitude ratios of spoofing signal to authentic. Simulation results on 10 data sets show that the probability of correct detection and mitigation is more than 90%.

Keywords: GPS, Cold-Start, Acquisition, Wavelet Transform, Hypothesis, Correlation
2020 MSC: 42C40, 62H20

1 Introduction

The power level of a normal Global Position System (GPS) signal is below the noise floor. Moreover, backward accordant technology along with a standard signal structure, makes it more vulnerable. A spoofer is a smart jammer that get GPS-like signals and deceives the receivers into generating fake time and position information. Several kinds of spoofing have been introduced. One general type spoofing attack changes the well-known standard data frame structure [9], where the spoofer gets a new fake data frame and reorders status bits to reject the incoming authentic GPS signals. Another kind of spoofing is generated by changing navigation and position levels. The spoofer inserts fake measurements into the receivers which affect the Position, Velocity, and Time (PVT) solution. Another approach for this mode of attack is based on known geometry relative to the target receiver that can extract the victim position and drag-off the authentic signal completely. This attack begins at low power and slowly rises till it can take control of the tracking loops. Finally, the authentic signal runs off in a self-consistent manner. In this type, the received signal strength is monitored by the Automatic Gain Control (AGC) block [13]. The other usual spoofing is named

*Corresponding author
Email addresses: moazedi@uma.ac.ir (Maryam Moazedi), m_mosavi@iust.ac.ir (Mohammad Reza Mosavi)

Received: December 2023 *Accepted:* February 2024

receiver-transmitter attacker, where the spoofing signal is synchrony with but stronger than the authentic signal [20]. Another fundamental type of spoofing signal is meaconing which get a replay of authentic GPS signals after a defined delay [14]. Existing different types of spoofing attacks provide much freedom in choosing the phasing of the signals and in injecting signals to a receiver without being detected [10]. The anti-spoofing methods are implemented into three layers [16]:

- Signal processing: These methods are presented in the field of tracking, including post-correlation [7], Wavelet Transform (WT), vector receivers, Maximum Likelihood Estimation (MLE), power analysis, and Minimum Mean Square Error (MMSE) [15]. However, these methods do not require additional hardware, the high volume of mathematical calculation leads to high computational complexity. Moreover, in these methods, the receiver must be locked with an authentic signal before start of the spoofing attack.
- Data bit: These methods commonly get additional hardware such as extra antennas for multi-antenna and Angle of Arrival methods [4]. Additionally, cryptographic methods require specific receivers and the signals that support cryptographic functions. Signal authentication methods such as digital signature, which track the existence of a random sequence in the signal code or navigation message [20], are also included in this category. These high-cost methods are not appropriate for mass production.
- Navigation data: Manipulated navigation bits are identified using: (1) navigation message analysis (scheduling of changes and NMA), (2) matching parameters changes (state variables) with models, and (3) consistency checks with navigation solutions [20].

Spoofer has to control and overcome all these levels to deceive the target receiver with a fake signal. An exhausted defense would contain spoofs at different levels in order to completely mitigate its effects. Generally, hardware-dependent strategies are powerful but high cost, while spoofing in signal processing needs no hardware. Moreover, studying different affected parameters in signal processing is easier. Along these lines, more number of researches in spoofing area get signal processing tools. From another aspect, three possible position is conceivable for a receiver during a spoofing attack [10].

- Cold-start: This situation is desirable for spoofer since the receiver cannot detect the fake signal unless with costly methods such as encryption and hardware-based approaches.
- Reacquisition: In this state, spoofing occurs before a warm start based on previous information. This is the operation basic of snap-shot receivers that have certain expectation of the received signal. Therefore, appearing any apparent inconsistency alarms a spoofing attack.
- Tracking: In this case, spoofing detection would be convenient through examining the disorderliness according to existing models [12].

Most of researches in spoofing field, deals with tracking segment of the receiver because of more probability of this state. However, it cannot be concluded that the acquisition is insignificant. Notably when a spoofer initially disables the receiver with blocking or jamming and imposes an initial reboot to the GPS receiver. One of main and accessible approaches of spoofing detection in all parts of receiver except cold start is checking for consistency during start of spoofing. This paper focuses on spoofing detection and mitigation in the cold start situation. The working principle of the proposed algorithm is based on multiple hypothesis tests on correlation peaks in acquisition in a way that spoofing signal with both lower and higher amplitude correspond to authentic signal will be studied The next section describes acquisition procedure in Software Defined Receiver (SDR). Afterward, the modified acquisition process based on a new decision rule is explained. Wavelet Transform (WT) based weak signal acquisition is also implemented here. The next Section, dedicated to explaining the utilized data benchmark for proposed algorithm evaluation, followed by simulation results. Then, some ideas for future work are noted. Finally, conclusions are provided.

2 Standard Acquisition in SDR

The transmitted civilian GPS signal consists L1 carrier modulated by navigation data and spread by the coarse acquisition (C/A) code. The received signal also consists additive noise and, possibly, interference. The receiver performs a code and carrier synchronization to estimate the corresponding unknown parameters, then follow despreading, demodulation and data detection. Certainly, the receiver should correlate the received data with infinite code shifts, which can be reduced by quantizing the uncertainty region into finite fragments or "bins". This is indeed the coarse

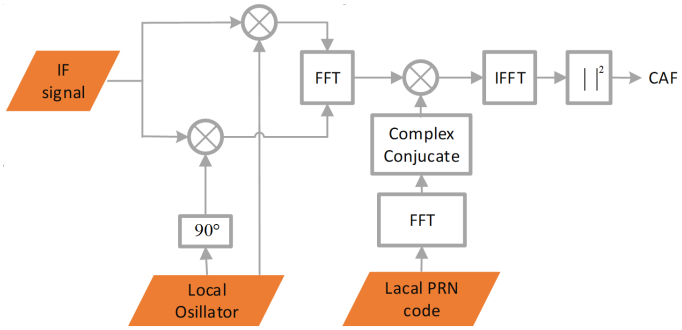

Figure 1: Block diagram of the parallel code phase search algorithm.The IF signal is multiplied by a local carrier signal to generate I and Q signals.The Fourier Transform of the input and the PRN code are multiplied, while the absolute value of time domain of the result represents the modulus of the correlation function between the input and the PRN code named CAF evaluated for a finite and discrete set of values of τ_i and $f_{d,i}$

synchronization or acquisition process. Then, a fine synchronization, named tracking [6], is performed by one of the available loops [13]. The Intermediate Frequency (IF) input digital signal of acquisition can be modeled as:

$$S_{IF}[n] = S(nT_S) = \sum_{i=1}^{Ns} AC_i(nT_s - \tau_i')D(nT_s - \tau_i')\cos(2\pi(f_{IF} + f_{d,i}')nT_s + \varphi_i') + W_{IF}(nT_S) \tag{2.1}$$

where N_S is number of satellites in view, T_S is the sampling interval, f_{IF} is the IF center frequency, A is the signal amplitude, C is the C/A code, $D(n)$ is the navigation message, φ_i' is a random phase, τ_i' is the estimated code delay, $f_{d,i}'$ is the estimated Doppler frequency, W_{IF} is a noise term [2].

During the acquisition, the receiver generates the local signal $C'(n)\exp(j2\phi f')$ and gets the signal power with non-coherent integrals (I and Q). The $I^2 + Q^2$ envelope is an important variance that from now will named Cross Ambiguity Function (CAF). In general, I and Q functions for each satellite are modeled with [11]:

$$\begin{cases} I \approx AD(n)R(\tau))\,\mathrm{sinc}(f_dT)\cos(\varphi) + \omega_I \\ Q \approx AD(n)R(\tau))\,\mathrm{sinc}(f_dT)\sin(\varphi) + \omega_Q \end{cases} \tag{2.2}$$

where $R(\tau)$ is the correlation function given by Eq. 3.2; τ is the interval of both the local code and the received code; T is the coherent time; f_d is the Doppler frequency; φ is the carrier phase; ω_I and ω_Q are additive white Gaussian noise (AWGN); and $\omega_I, \omega_Q \sim N(0, \sigma^2)$.

$$R(\tau) = \begin{cases} \tau + 1, -1 \leq \tau < 0 \\ -\tau + 1, 0 \leq \tau \leq 1 \quad r \\ 0, others \end{cases} \tag{2.3}$$

Three available methods for correlation extraction are: (1) serial search with calculating time domain correlation, (2) parallel search in carrier frequency with Fast Fourier Transform (FFT) [22], and (3) parallel search of code phase with FFT. Figure 1 shows the utilized SDR with the third search method [3]. Initially, input signal is multiplied by a locally generated carrier signal. The I and Q signals are generated through multiplication with sine signal and a 90◦ phase-shifted version of that, respectively. To get a circular correlation through Fourier transforms, complex conjugate of generated PRN code in the frequency domain is multiplied with the FFT of the input. The result of the multiplication is transformed into the time domain by an inverse Fourier transform that represents the correlation between the input and the PRN code.

The next task of the acquisition is the decision-making based on the specific statistical tests. The performed test utilized in the standard SDR is defined as:

$$\begin{cases} H0 = \frac{P_2}{P_1} < Tr \\ H1 = \frac{P_2}{P_1} > Tr \end{cases} \tag{2.4}$$

where *H0* and *H1* relates to invisible and visible satellites, respectively. *P1* and *P2* are, respectively, the first and second peak of envelope function. Pseudocode of peak extraction in SDR has been reported as:

```
%"Remove carrier" from the signal
I = sinCarr. * signal;
Q = cosCarr. * signal;
%Convert the baseband signal to frequency domai
IQfreqDom = fft(I + j * Q);
%Multiplication in the frequency domain (correlation in time domain)
convCodeIQ = IQfreqDom. * caCodeFreqDom;
%Perform inverse DFT and store correlation results
acquisitionResults = abs(ifft(convCodeIQ)).^2;
%Find the correlation peak and the carrier frequency
[P1 frequencyBinIndex] = max(max(acquisitionResults, [], 2));
%Find code phase of the same correlation peak
[P1codePhase] = max(max(acquisitionResults));
%Find 1 chip wide C/A code phase exclude range around the peak
RangeIndex1 = codePhase - samplesPerCodeChip;
RangeIndex2 = codePhase + samplesPerCodeChip;
%Correct C/A code phase exclude range if the range includes array boundaries
codePhaseRange = [1 : RangeIndex1, RangeIndex2 : samplesPerCode];
remainedSignal = results(frequencyBinIndex, codePhaseRange);
%Find the second highest correlation peak in the same freq. bin.
P2 = max(remainedSignal);
```

If the related PRN is not visible, both*P1* and*P2* will be noise-related, and their ratio will be valued less than Tr. Otherwise,*P1* and*P2* will be proportional to the signal power and noise level, respectively. For the satellites with two correlation peaks (authentic and fake) in their CAF,*P1* and*P2* would still be close to each other. Therefore, they will be excluded due to the smallness of (P1/P2), and only PRNs with one peak (authentic or fake) could be detected. On the other hand, stating a spoofing attack could generate additional correlation peaks which may increase the noise floor in the GPS receiver. To mislead the acquisition procedure, the spoofing correlation peak must be more powerful than the authentic one. However, the cross correlation terms caused by lower power spoofing signals can decrease the noise floor of the receiver and consequently elevate the effective Carrier to Noise Ratio (CNR) of authentic signals to mislead the acquisition process into estimating an incorrect peak and reducing the detection performance. The authors are concentrated on the evaluation of effects caused by spoofing signals in the acquisition of a civil GPS receiver. The novelty of this article is providing a solution for this fundamental problem in the SDR that hereafter referred to the smart acquisition.

3 Modified Immune Acquisition against Spoofing

Because of the variability and complexity of intentional interferences, it is very difficult for one single anti-spoofing approach to properly treat all spoofing modes [5]. The proposed method nearly ensures security of the acquisition segment against 10 spoofing data sets. Firstly, the spoofing signal model is defined this section. Then, the steps of the proposed algorithm will be explained in detail. A short discussion about threshold comes at the end.

3.1 Signal Model

The received signal in the presence of a spoofing signal is simply modeled as:

$$S_{in}[n] = \beta[S_A(n) + \alpha S_F(n-d) + \omega(n)] \tag{3.1}$$

where $\alpha = 10^{FAR/20}$ represents the amplitude ratio, FAR indicates the fake to authentic signal ratio in dB, and β is the AGC gain at the front end which affects the entire received signal.d is the spoofing signal delay with respect to the authentic signal. Finally, S_A and S_F represent authentic and spoofing signals, respectively. Initial models assume a very sharp peak for CAF while its sidelobes are completely buried by the noise terms. Indeed, this approximation is not exact because of the presence of non-zero correlation values, and a more accurate model accounting these imperfections should be considered. Envelope comparison of spoofing and authentic signals indicates that spoofing attack can be recognized by a double statistical test [6]:

$$\begin{cases} H0H0(no\ signal) : CAF \approx (\mu + w_I)^2 + (\mu + w_Q)^2 \\ H1H0(single\ signal) : CAF \approx (AR(\tau)\,\mathrm{sinc}(f_d T))^2 + (\mu + w_I)^2 + (\mu + w_Q)^2 \\ HxH1(double\ signal) : CAF \approx A^2\,\mathrm{sinc}(f_d T)(R(\tau)^2 + \alpha^2 R(\tau - \Delta c)^2 \\ +2\alpha R(\tau)R(\tau - \Delta c))\cos(\varphi' - \varphi) + (\mu + w_I)^2 + (\mu + w_Q)^2 \end{cases} \tag{3.2}$$

where $H0H0$, $H1H0$ and $HxH1$ means that no signal, one single signal and two signals are available, respectively. Δc is the signal's interval between the counterfeit and the authentic signal and can be either positive or negative. φ' is the carrier phase of the counterfeit signal. When the interval is very small, they are completely synchronous, and the carrier phase's interval is approximately 0, i.e., $\cos(\varphi' - \varphi) \approx 1$. Otherwise, when the signals intervals is more than 2 code phase the carrier phase's interval is a factor. Regardless of its value, two peaks would be founded. The cells close to the main peak are significantly affected by the signal presence that we named secondary peaks. In order to account the effect of these peaks, an enhanced Gaussian model has been tested: all the simulated Gaussian random variables present a mean equal to μ, except the ones representing main peak and the four adjacent cells. The means of the four adjacent cells were set to the values measured on the squared root of a noiseless search space. Commonly, noise threshold is selected based on the acceptable probability of false acquisition and noise spectral power density [9] as:

$$N - Tr = -2\sigma_N^2 \ln[1 - (1 - P_{FA})^{\frac{1}{N_C}}] \tag{3.3}$$

where N_C is the length of the processed signal, and P_{FA} is the probability of false acquisition. The noise variance can be shown as:

$$\sigma_N^2 = E[W_{IF}^2(t)] = N_0 B_{IF} \tag{3.4}$$

where $N_0/2$ is the power spectral density of the IF noise, and B_{IF} is the front-end bandwidth. Secondary peaks are present because of correlation side values which are considered by the mean factor μ introduced in 3.2. Therefore, the noise threshold is optimally determined by:

$$N - Tr = -2\sigma_N^2 \ln[(1 - (1 - P_{FA})^{\frac{1}{N_C}})/(\sum_{K=0}^{\infty} (\frac{\mu}{\sqrt{Tr}})^K I_K(\frac{\mu\sqrt{Tr}}{\sigma_N^2}))] - \mu^2 \tag{3.5}$$

where $I_K(.)$ is the modified Bessel function of the first kind of K order [2].

3.2 The Principle of the Proposed Method

The standard receiver performs a single hypothesis tests and reports the corresponding single PRN peak and hands over its parameters to the tracking loop. However, a smart acquisition considers the possibility of another state in which the spoofer has induced a fake peak for the related PRN. This proposed smart acquisition in this work can not only detect but also identify spoofing signal. Figure 2 elaborates the flowchart of implementation details to separate the spoofing peaks. Hereafter, a more detailed explanation is provided:

Step 1: The first thing that algorithm should focus on is calculation of correlation as shown in Figure 1. In the presence of spoofing, it will be:

$$N - Tr = R(\tau, f) = R_A(\tau, f) + \alpha R_F(\tau - \Delta\tau, f - \Delta f) + N \tag{3.6}$$

where A and F denote the authentic and spoofed fake signal, respectively. $\Delta\tau$ and Δf are the time delay and the frequency difference relative to authentic signal, respectively.

Step 2: The Function *Sub1* in the Figure 2 extracts the first peak (PA) and the second peak (PB) of the input signal in the way that explained in the above mentioned pseudo code; subsequently the equations of $PA = P1$ and $PB = P2$ are set. Then, $P1/P2$ is compared with the acquisition threshold. A ratio larger threshold means *H1* is true. Classification process of peaks is performed during total algorithm as explained in next steps.

Step 3: As a smart acquisition, to detect whether the extracted peak is authentic or fake, a second hypothesis test after a WT-based denoising process is applied to the remained signal (sea the pseudo code). In other words, Sub1 function is applied again to extract the *PA* and *PB* values of denoised signal. Afterward, the hypothesis test is done. As can be seen in the figure 2, in this step, *PA* and *PB* are indeed *P2* (second peak) and *P3* (third peak) of the initial signal, respectively. Detection of a new peak, evidences a spoofing attack (H1H1); otherwise, the initial peak will be considered as an authentic peak (H1H0). Denoising gets the wavelet coefficients so that the related coefficients of the noise are considered zero to remove them from the initial signal. The product of the wavelet and the noise is numerically small since the noise spectrum is extended at all frequencies. On the contrary, most of the signal information is available on a small number of coefficients, making the amplitude of these coefficients large; thus, the signal will not be damaged by denoising with these three stages: 1. Applying a signal with a length of N to a selected wavelet at the K level. 2. Determining the threshold for separating the coefficients such that the noise is eliminated. 3. Using the coefficients for the inverted wavelet and extracting the main noise-free signal. To have effective

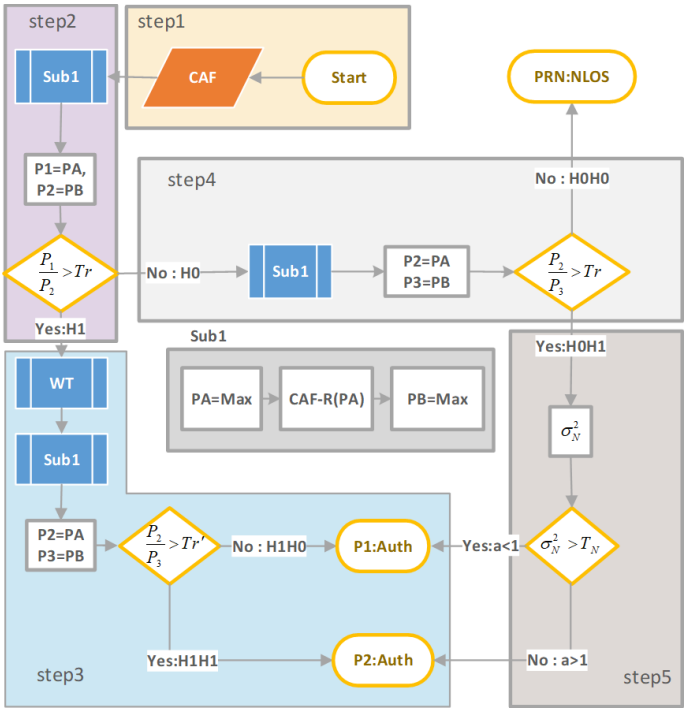

Figure 2: Flowchart of proposed spoof detection and reduction multiple hypothesis algorithm. The hypothesis test for peak detection is performed two times. Therefore, four states are possible; H0H0 and H1H0 represent no signal and single peak, respectively. In the other two states, HxH1, two peaks are detected. The fact that the single peak is authentic or not is identified by WT . Which one of the double peaks is authentic is also answered with proper criteria in second hypothesis test.

denoising through wavelet, the proper selection of components is significant. For example, selecting the appropriate base function, then accurately determining the number of decompositions (K), and most importantly, selection of an optimal threshold is necessary. For this purpose, the proposed method in the study of [18] is applied by factorizing differential acquisition. The more similar mother wavelet with the original signal gives the better decomposition. The rbio1.1 mother wavelet from the reverse biorthogonal family introduced by [19] is utilized that is well compatible with the GPS signal. In order to increase the probability of detecting the available potential signal, the maximum number of decomposition levels equal to the following equation has been selected:

$$K_{MAX} = \lfloor \log_2 N \rfloor \tag{3.7}$$

where N is the length of the processed signal. The resolution threshold is determined based on the statistical characteristics of the processed signal according to:

$$\lambda_{i,j} = \mu_i + K_{i,j}\sigma_i \tag{3.8}$$

where $K_{i,j}$ is an adjustable parameter to manipulate the effect of non-zero bias in threshold determination. Furthermore, μ_i and σ_i respectively represent the average and standard deviation of detail components in each level of decomposition and can be expressed by:

$$\mu_i = \frac{\sum_{j=1}^{N_i} w_{i,j}}{N_j}, \ \sigma_j = \sqrt{\frac{1}{N_i - 1}\sum_{j=1}^{N_i}(w_{i,j} - \mu_i)^2} \tag{3.9}$$

where $w_{i,j}$ are the WT coefficients, and navigation section N_i indicates the number of elements in each detail component. After obtaining the threshold and removing the coefficients below its level, the signal reconstruction stage with the remaining coefficients is performed, which results in a noise-free signal. Since this algorithm is performed in cold start of acquisition stage, computation cost is very low and. The whole algorithm performs only in some seconds.

Step 4: If the initial hypothesis is not proved (H0). In the case of a standard receiver, it means that the satellite is invisible. However, for a smart acquisition, a second possibility is considered. This is the above mentioned main problem of SDR in acquisition when *P1* and *P2* are correspond to the authentic and spoofing signal with about close signal amplitudes. This can be distinguished among another hypothesis where the *Sub1* function is rerun on the

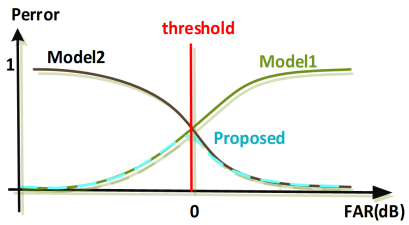

Figure 3: Qualified comparison of proposed spoof detection with previous models. Model 1 assumes that the authentic signal is stronger than the spoofing signal, and vice versa in model 2. The proposed model decision depends on the estimated AGC coefficient. If β is less than the threshold, the higher peak relates to the authentic signal, otherwise it relates to the spoofing signal.

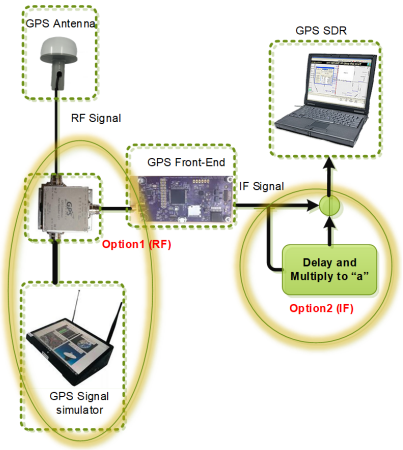

Figure 4: Implemented lab platform for data collection. The spoof data is generated in two ways. First, the input RF signal is combined with simulators output in the hardware platform. Second, the combination of IF signals is performed in the software platform.

remained signal. Then, the $P2/P3$ ratio is compared with the acquisition threshold; a small ratio means that they are close to each other and belong to the noise signal and this PRN is actually invisible (H0H0). Otherwise, a new peak is identified (H0H1). The next step dedicates to determine whether *P1* is authentic or *P2*.

Step 5: The spoofing signal is usually higher than the authentic signal, but not always. Moreover, at the initial stage of the synchronous intermediate spoofing α is less than one. Generally, separation of spoofing and authentic close peaks is an essential challenge in the spoofing field. In this research the authors have solved this problem by concentrating on the effect of AGC gain (β). In is obvious that high power spoofing signal ($\alpha > 1$) needs smaller β. Since β in the Eq.3.1, is also applied to noise, the noise level in case of $\alpha > 1$ is lower than the case of $\alpha < 1$; Referring to [8] β can be extracted from IF signal as the filter. According to these points, selecting an appropriate threshold for β, the range of α value can be estimated. In the other words, if $\beta > \beta_{trh}$, then $\alpha < 1$ and *P2* indicates an authentic peak; otherwise, the *P1* will be considered as the authentic peak. Qualitative analysis of this decision-making pattern is demonstrated in Figure 3. The probability of decision-making error is presented in three decision rules: (1) higher peak related to authentic signal, (2) higher peak related to spoofing signal, and (3) the proposed model. It can be observed that in the case of the correct estimation of the threshold, the cumulative error of the proposed algorithm is considerably lower.

4 Dataset Benchmark

As stated in the literature, it is actually impossible to get an exhaustive platform for spoofing experiments tests, and it is illegal to spread spoofing signals outdoor. Here, a data set of various spoofing data was exploited for performance evaluation. This data set, covers two main kinds of spoofing contain SDR and relay spoofing. As can be observed in Figure 4, the spoofing signal enters from two directions to the GPS receiver: (1) input as RF and (2) it is combined with an authentic signal in the IF domain after the front-end section. The first case often occurs in actual spoofers. However, the second case is more appropriate for research applications since it allows studying all of the parameters. The essential difference between the two cases is passing the RF signal from the AGC. In the case of the RF domain, the spoofing signal has passed the AGC while accompanied by the main signal and noise. The resultant signal power

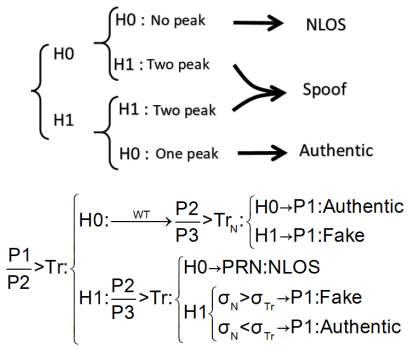

Figure 5: Summarize of the multiple hypothesis: (top) detection (bottom) reduction.

has been adjusted according to its maximum peak. Here, the analyses have been carried out on IF data; nevertheless, the ultimate assessment was performed on the RF data sets. The replay spoofing attacks are available in both the RF and IF domains in the utilized benchmark. In the implemented platform in the IF domain [1], the satellite data are collected through a GPS antenna for a specific duration; afterward, they are applied to the front-end section. In this section, the input signal is initially reinforced by a Low-Noise-Amplifier. Subsequently, it is sampled at a 5.714 MHz rate and converted to two bit digital signal through 4 levels of $\pm$ 1 and $\pm$ 3, which is applied to the software platform in MATLAB in the form of *.bin file [3]. The received signal was delayed in the SDR input by various durations and was added to the main signal with different amplitude coefficients. The achieved signal was applied to the improved SDR with the proposed algorithm as the spoofing data, and the results were assessed. If the main signal is modeled through (1), the spoofing signal is represented by:

$$S_{(spoof)} = A_S C_S(n) D_S(n) \cos(2\pi f_s n + \varphi_S) \tag{4.1}$$

where S represents spoofed fake signal. Various types of spoofing are obtained by changing the parameters A, C, D, f_S and φ_S respective to authentic signal. It has been attempted in the second data set to compensate for the quantization error of the analog to digital converter in the front-end by combining the authentic and fake signals in the RF domain. According to the authors' available laboratory facilities, this step can be solely realized through a GPS signal simulator. This procedure combines the simulator-produced signal with one from a rooftop GPS antenna and further applies the resulting data to the front end. All of the cases were implemented through various amplitude and delay values. To test the proposed approach in a more realistic state, semi-dynamic spoofing is also generated as a third data set, where the authentic signal is related to a moving car with constant velocity, and the attacker sends its GPS position signals toward the target receiver. In other words, the target receiver is mobile, but the spoofer is static. Finally, in the most real case, both the authentic and spoofing signals are dynamic. The target receiver is moving in the right path, but the spoofer tries to deviate that in the middle of the route. All processing was done on a laptop ASUSK46C with i5 1.8 GHz CPU. In this regard, more than 200 different data were generated. Moreover, 6000 different CAF outputs were approximately extracted for the acquisition stage. Through this process, the different states spoofing signal power can be generated.

5 Simulation Results

Due to the fact that extracting precise equation of the algorithm performance is challenging, various conditions have been evaluated by the simulation to show the validity of the algorithm. As shown in Figure 5, the algorithm achievement can be investigated in two different phases: (1) correct recognition of the spoofing presence (detection) and (2) correct distinguishing between authentic and fake peaks (reduction). If the received signal is accompanied by a spoofing signal and the proposed method can correctly detect the spoofing presence and its features, it can be stated that the algorithm has succeeded. While, reduction failure mostly occurs once the noise level and the FAR coefficient are not correctly estimated, which happens more likely at values close to $FAR = 0dB$.

The Receiver Operating Characteristic (ROC) output was separately illustrated, in addition to the overall algorithm for various decision-making stages. The ROC curve has been presented to evaluate the initial decision rule for peak presence or absence states. Results for the standard receiver for various $P1/P2 = Tr$ have been illustrated in Figure 6. To get at a higher assurance, the error percentage that is the summation of the two error types, the probability of false alarm (Pfa), and probability of missed detection (Pmd), is demonstrated separately for various Tr values (Figure7). Considering both diagrams validate the optimum value of 4.7 for Tr.

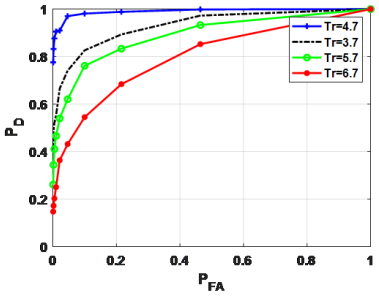

Figure 6: Performance evaluation versus threshold value in standard acquisition. Tr=4.7 is the best decision with less error.

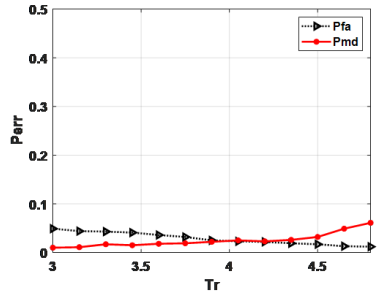

Figure 7: Probability of spoof detection error versus threshold. The proposed algorithm has best performance in Tr=4.7.

In the case of determining the noise threshold for peak selection in (H1H1), Figure 8 represents the comparison between ROCs obtained with the standard and the enhanced model. As can be seen, results prove the impact of adjacent cells. Finally, in Figure 9, the ROC of the overall algorithm is demonstrated for various FARs; if the spoofing signal power is higher than 15 dB, the attenuation rate of AGC will be high, and the remaining authentic signal will not be distinguishable by WT. Acquisition parameters during simulation in SDR are shown in Table 1.

Additionally, in Figure 10, the acquisition result for the dynamic spoofing data with $FAR = 12dB$ is presented in the bar chart. The PRNs in which $P1/P2 > 4.7$ are indicated by green color, and the rest are represented in blue. Signals of PRN 4 and PRN 27 will be investigated in more detail in Figures 11, 12 and 13. In PRN 22 the authentic peak is extracted by WT (H1H1). In PRN4, it is extracted by fake peak removal (H0H1). Classification performance can be investigated in a 2×2 Confusion Matrix (CM), including True Positives (TP), False Positives (FP), False Negatives (FN), and True Negatives (TN), where positive means authentic PRNs and negative means fake PRNs. Therefore, TP is the number of correctly detected authentic peaks, and TN is the number of correctly detected fake peaks. The FP shows falsely detected authentic peaks. Eventually, FN relates fake peaks that are detected falsely,

$$CM = \begin{pmatrix} TP & FP \\ FN & TN \end{pmatrix} = \begin{pmatrix} 971 & 26 \\ 47 & 4956 \end{pmatrix} \tag{5.1}$$

where the rows (1) and (2) report authentic and spoofed peaks respectively and off-diagonal elements are related to wrong detections.

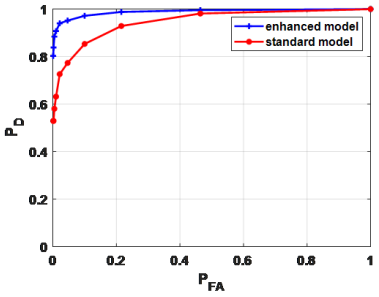

Figure 8: Performance evaluation of peak selection in CAF. Detection error seriously depends to selected noise level.

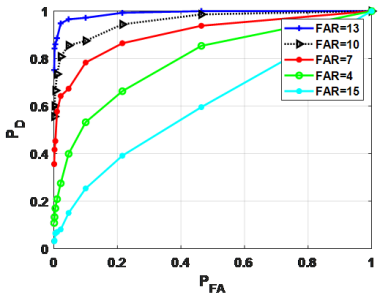

Figure 9: ROC of proposed algorithm based on FAR. Best performance is in FAR=13

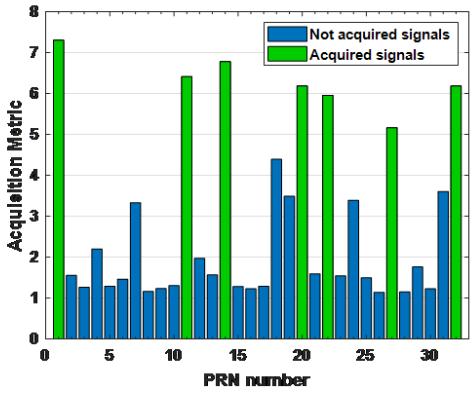

Figure 10: Acquisition result for the dynamic spoofing data with FAR=12dB. The green color indicates the acquired PRNs with high peak ratio, and the rest are represented in blue.

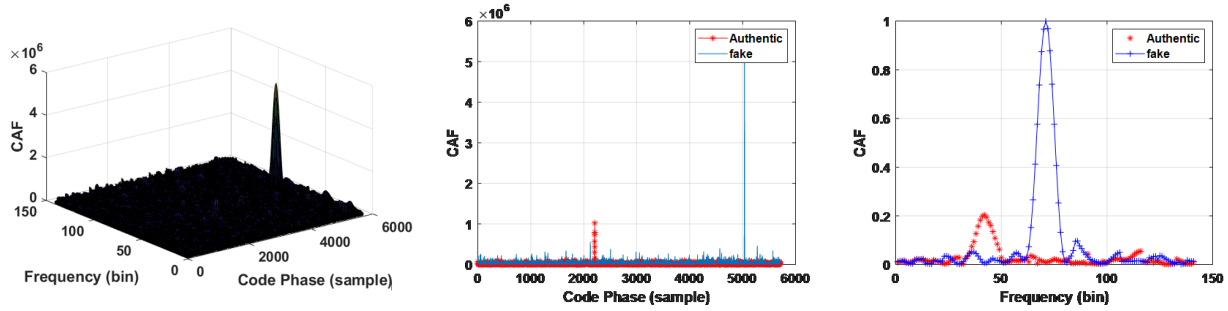

Figure 11: CAF for PRN22: (top) surface of initial state, (middle) versus code phase at carrier frequencies, (bottom) versus carrier frequency at code phase.

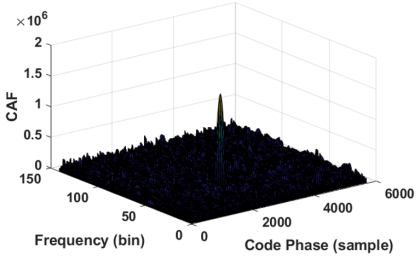

Figure 12: Extracted authentic peak of PRN22 after WT denoising.

Table 1: Acquisition parameters during analysis.

IF (f)	1.405396825 MHz
Sampling f	5.714 MHz
Intermediate, sampling and code frequencies	1.023 MHz
non coherent integration time	11 ms
Number of PRNs to be search	32
List of PRNs to be	8
Code length	1023 Chips
Search space	100 Hz , 0.17 chip

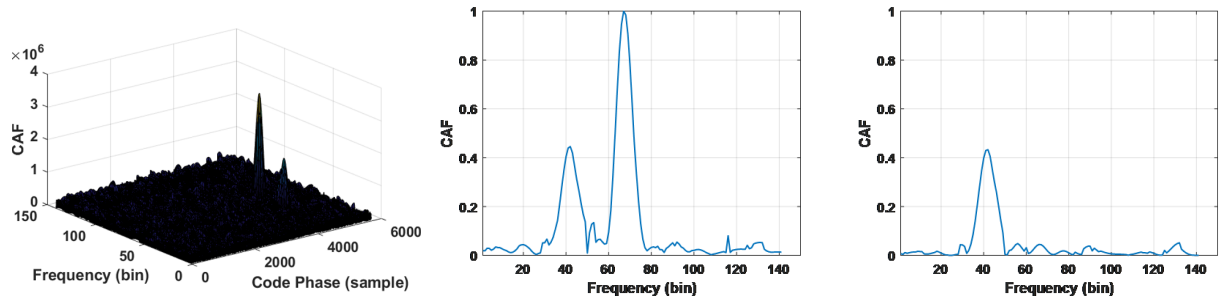

Figure 13: CAF for PRN4: (top) surface of initial state, (middle) versus code phase at carrier frequency, (bottom) Extracted authentic peak after fake peak removal.

It can be noted that the FN parameter is represented by a relatively high value. This means that the algorithm cannot precisely detect fake peaks. To address the issue, the processing steps of SDR have been performed and the significant parameters have been reported in Table 2. The right column corresponds to the reduction percentage of spoofing error in the spatial dimension after applying the algorithm. The separate CM values and the DOP parameter have been reported to examine each data status. It can be noted that the FN and DOP values are high for data sets (3, 5 and 9) in which the reduction percentage of spoofing error is low. Through a more accurate examination, it has been indicated that several fake PRNs are actually invisible satellites. Moreover, there is no authentic signal in the CAF output for that PRNs, and the algorithm cannot detect them. On the other hand, as can be clearly observed in the DOP column, the DOP parameter has been reported significantly high for these data. It can be concluded that spoofing PRNs that are not detectable by the algorithm are invisible satellites, which disturb the constellation and can be conveniently detected through the navigation section of the receiver. For validation of this result, the navigation process was performed once more by removing these PRNs. The result of this process data reported in Table 3. As can be noted, the error reduction percentage has been increased by 30% on average. The worst route with the most computational volume has been considered to measure the computational complexity. The search step is one of the parameters that significantly contribute to the computational volume. The calculations were repeated in four different

Table 2: Algorithm performance for different data sets.

Data Set	Spoof kind	DOP	TP	FP	TN	FN	Spoof error (m)	Spoof reduction (%)
1	Static (IF)	4	3	0	6	0	88	94
2	Static (IF)	6	3	0	5	0	321	89
3	Static (IF)	13	0	1	4	3	65	57
4	Static (IF)	5	2	1	5	0	342	85
5	Static (IF)	26	2	0	2	4	98	45
6	Static (IF)	3	3	0	7	0	254	92
7	Semi-dynamic	7	4	1	4	1	87	78
8	Semi-dynamic	6	3	1	1	2	93	72
9	Dynamic	15	3	2	2	3	178	65
10	Dynamic	5	4	1	3	0	545	87

states, and the algorithm efficiency and computational cost were extracted. The evaluation results are demonstrated

in Table 4. To separate the best state, a Figure of Merit (FOM) is introduced as:

$$FOM = \frac{ToS}{Max(ToS)} \times \frac{Max(p_e)}{P_e} \tag{5.2}$$

where ToS denotes the time of process and Pe is error probability. It can be seen that state (3) is an appropriate selection in case of joint consideration of efficiency and computational volume.

Table 3: Algorithm performance for some datasets after removal of high DOP PRNs.

Data Set	Spoof kind	DOP	TP	FP	TN	FN	Spoof error (m)	Spoof reduction (%)
2	Static (IF)	6	0	1	4	0	65	84
5	Static (IF)	2	2	0	2	0	98	75
10	Dynamic	3	3	2	2	0	178	95

Table 4: Time complexity in different search spaces.

State	$\Delta Codephase$ (Chip)	ΔF(Hz)	Pe (%)	ToS(mSec)	FOM
1	0.1	100	7.5	22.543	3.11
2	0.1	150	12	16.964	1.73
3	0.17	100	9	15.7	3.41
4	0.17	150	16	8.4	2.68

5.1 Comparison with previous works

In Table 5, the performance of smart acquisition was compared against some well-known methods [17] in different parts of the receiver. We get a numerical value from 0 to 10 to each feature for the worst to the best state, depending on the algorithm performance. For example, regarding the "necessary equipment" feature, an algorithm takes 10 if no extra equipment is needed. Besides, in case of necessity to basal changes in receiver structure, it earns 0. Since acquisition is the first step of GPS baseband signal processing, countering at this point is timely and more affective. Yuan and co-authors [21] have also performed their method in cold-start, but only in generative spoofing and theoretical space. Multimodel detection [11] has performed the searching process while the acquisition does not need to find new PRNs. Moreover, it is only evaluated theoretical. Overall, the proposed algorithm performs better than the other ones because of following advantages: Firstly, it needs no extra hardware. Secondly, mitigation is performed timely and simultaneously with detection in first step of navigation (cold-start). Thirdly, it covers all states of spoofing power relative to power of authentic signal.

5.2 Future Work

In the future study, other interferences, such as multipath and jamming, will be addressed by combining the smart acquisition with other data processing methods included. The difference in jamming is in the power of detecting a fake peak or peaks. Just by detecting jamming, the receiver is put into an alert mode, and it does not trust the channels that are flagged as impaired. For multipath, three significant distinctions can be noticed. The first is that the amplitude of the multipath signal is usually less than the main signal amplitude. The second is its delayed phase with respect to the main signal, and the last point is the insignificant code phase difference with the main signal. Moreover, this algorithm will be tested on new datasets containing other types of attacks to optimize the performance and will get a better criterion for the empirical thresholds. Using noise discussion in [7], a more detailed model for getting threshold will be presented. A most important work can be updating the tracking loop PRNs with parameters of authentic signal instantly, because cold-start module is unused when all channels of the receiver are tracing signals. In other words, this algorithm can be extended easily to counter tracking loop attacks.

Table 5: Comparing some anti-spoofing methods and proposed smart acquisition.

Detection methods	Analyzed features	Required equipment	Advantages	Limitations	Total mark
Spatial processing [4]	The direction of signal entry to receiver (6)	Array antenna and software upgrade (2)	High reliability and not need prior data (8)	The high cost and inefficiency of and multiple antennas (2)	18
NMA [20]	Navigation (3)	Military receivers (1)	Reliable (6)	Inefficient in civil receivers (1)	11
C/N0 [5]	Carrier-to-noise ratio (5)	Hardware for measurement (2)	Simplicity (5)	Unreliable in synchronous attacks and the spoofer power control (2)	14
SQA [7]	Correlation branch (4)	Software upgrade (6)	short effective time, easy to implement, real-time (6)	warm-start,only theory and detection (2)	17
Multi Mode [11]	Correlation branch (4)	Software upgrade (6)	short effective time, easy to implement, real-time (6)	warm-start,only theory and detection (2)	18
Joint detect [21]	Consistency of code and carrier (5)	Software upgrade (6)	Not need prior data, easy to implement, cold start, , real-time,Detection and mitigation (7)	Inefficient in repeater spoofing, only theory, special case (2)	19
This work	Correlation in Acquisition (5)	Software upgrade (6)	No need prior data, easy to implement, cold start , real-time, cover all states of spoof power Detection and mitigation (8)	only simulation (3)	22

6 Conclusion

The hypothesis test introduced as a tool for interference detection has been revisited and improved to tailor it to spoofing countering at cold-start by searching for a possible second peak in various conditions. In the case of detecting a mere single peak in the first hypothesis, the existence of a possible attenuated second peak is investigated through applying wavelet transform on the residual signal. It has been demonstrated that the algorithm can correctly detect with a probability of above 90%. The main innovation of this research is taking countermeasure against spoofing in the cold-start of the GPS receiver only by signal processing and without requiring encryption or hardware-based methods; this makes that appropriate for mass production. More importantly, the receiver requires no prior information. Additionally, the receiver can use this method when the spoofing imposes a reacquisition to the receiver for its success. In the real and snap-shot receivers that new leak-in satellites are consecutively searched, using this method will considerably increase the efficiency and reliability of the receiver. Furthermore, an extensive set of spoofing data has been utilized to evaluate the proposed method. Ultimately, the proposed method is regarded as a suitable option for real-time applications due to its simplicity and low computational volume.

References

[1] A.R. Baziar, M. Moazedi, and M.R. Mosavi, *Analysis of single frequency GPS receiver under delay and combining spoofing algorithm*, Wireless Person. Commun. **83** (2015), 1955–1970.

[2] D. Borio, L. Camoriano, and L.L. Presti, *Impact of GPS acquisition strategy on decision probabilities*, IEEE Trans. Aerospace Electronic Syst. 44 (2008), no. 3, 996–1011.

[3] K. Borre, D.M. Akos, N. Bertelsen, P. Rinder, and S.H. Jensen, *A Software-Defined GPS and Galileo Receiver: A Single-Frequency Approach*, Springer Science and Business Media, 2007.

[4] A. Broumandan, A. Jafarnia-Jahromi, S. Daneshmand, and G. Lachapelle, *Overview of spatial processing approaches for GNSS structural interference detection and mitigation*, Proc. IEEE **104** (2016), no. 6, 1246–1257.

[5] F. Dovis, *GNSS Interference Threats and Countermeasures*, Artech House, 2015.

[6] E. Garbin Manfredini and F. Dovis, *On the use of a feedback tracking architecture for satellite navigation spoofing detection*, Sensors **16** (2016), no. 12, 2051.

[7] Y. Hu, S. Bian, K. Cao, and B. Ji, *GNSS spoofing detection based on new signal quality assessment model*, GPS Solutions **22** (2018), 1–13.

[8] A. Jafarnia Jahromi, *GNSS signal authenticity verification in the presence of structural interference*, PhD diss., University of Calgary, 2013.

[9] E.D. Kaplan and C.J. Hegarty, *Understanding GPS: Principles and Applications*, Norwood, MA: Artech House, 2017.

[10] F. Lazaro, R. Raulefs, H. Bartz, and T. Jerkovits, *VDES R-Mode: Vulnerability analysis and mitigation concepts*, Int. J. Satellite Commun. Network. **41** (2023), no. 2, 178–194.

[11] M. Li, Y. Yuan, N. Wang, Z. Li, Y. Li, and X. Huo. *Estimation and analysis of Galileo differential code biases*, J. Geodesy **91** (2017), 279–293.

[12] C. Liang, M. Miao, J. Ma, H. Yan, Q. Zhang, and X. Li, *Detection of global positioning system spoofing attack on unmanned aerial vehicle system*, Concurren. Comput.: Practice Experience **34** (2022), no. 7, e5925.

[13] A. Polydoros, *On the synchronization aspects of direct-sequence spread spectrum systems*, Ph.D. dissertation, Department of Electrical Engineering, University of Southern California, 1982.

[14] S. Semanjski, I. Semanjski, W.D. Wilde, and A. Muls, *Use of supervised machine learning for GNSS signal spoofing detection with validation on real-world meaconing and spoofing data—Part I*, Sensors **20** (2020), no. 4, 1171.

[15] E. Schmidt, Z. Ruble, D. Akopian, and D.J. Pack, *Software-defined radio GNSS instrumentation for spoofing mitigation: A review and a case study*, IEEE Trans. Instrument. Measurement **68** (2018), no. 8, 2768–2784.

[16] E. Schmidt, Z.A. Ruble, D. Akopian, and D.J. Pack, *A reduced complexity cross-correlation interference mitigation*

technique on a real-time software-defined radio GPS L1 receiver, IEEE/ION Position, Location and Navigation Symposium (PLANS), IEEE, 2018, pp. 931–939.

[17] E. Shafiee, M.R. Mosavi, and M. Moazedi, *Detection of spoofing attack using machine learning based on multi-layer neural network in single-frequency GPS receivers*, J. Navigation **71** (2018), no. 1, 169-188.

[18] M. Sharie, M.R. Mosavi, and N. Rahemi, *Acquisition of weak GPS signals using wavelet-based de-noising methods*, Survey Rev. **52** (2020), no. 375497–375513.

[19] M. Sharie, M.R. Mosavi, and N. Rahemi, *Determination of an appropriate mother wavelet for de-noising of weak GPS correlation signals based on similarity measurements*, Engin. Sci. Technol.: Int. J. **23** (2020), no. 2 281–288.

[20] Z. Wu, Y. Zhang, and R. Liu, *BD-II NMA and SSI: An scheme of anti-spoofing and open BeiDou II D2 navigation message authentication*, IEEE Access **8** (2020), 23759–23775.

[21] D. Yuan, H. Li, F. Wang, and M. Lu, *A GNSS acquisition method with the capability of spoofing detection and mitigation* Chin. J. Electron. **27** (2018), no. 1, 213–222.

[22] L.I. Yang-zhi, L. Guangxia, and C. Jian, *The research and modification of the cascaded FFT acquisition algorithm*, Signal Process. **27** (2011), no. 5, 721-726.