IUST
Iran University of Science and Technology

Iranian Journal of Electrical and Electronic Engineering

Journal Homepage: ijeee.iust.ac.ir

An Anti-spoofing Algorithm using a Kalman Filter based ARAIM Algorithm

M. Moazedi* (C.A.), M. R. Mosavi** and D. M. De Andrés***

Abstract: The Receiver Autonomous Integrity Monitoring (RAIM) method uses additional information to detect and remove spoofing signals by analyzing pseudo-range measurements. Therefore, assuming that spoofing signals are errors for the valid signal, RAIM can be a practical method that does not impose expensive hardware to the receiver. Typically, RAIM operates under the assumption that simultaneous multi-satellite errors are highly unlikely. For example, GPS satellite errors occur no more than three times per year. Some enhanced RAIM methods have been proposed in recent years that employ additional measurements, such as Doppler shift measurements, time-differential carrier phase measurements, and so on. Since simultaneous multiple fake satellites are common in spoofing cases, basic RAIM cannot counter these types of signals, and for eliminating more than one spoofing or error signal requires additional information, such as measurements on other frequencies or satellite systems, which increases the complexity of execution. In this paper, an anti-spoofing method based on Advanced RAIM (ARAIM) has been proposed with a novel slope-based RAIM availability assessment method. Simulation results on several spoofing data sets indicate the definitive success of the proposed methods in detecting and mitigating spoofing error, with a detection success rate of over 79% using the statistical method and over 87% using the Kalman filter method.

Keywords: Anti-spoofing, GPS, Kalman Filter, RAIM.

1 Introduction

THE Receiver Autonomous Integrity Monitoring (RAIM) was the first method that FAA adopted to ensure Global Positioning System (GPS) monitoring, deeming it essential for civilian GPS usage [1]. Since 1992, RAIM has been considered a fundamental part of airborne electronic systems and is primarily used to detect satellite errors based on pseudo-range measurements. Extensive experimental and theoretical work has been conducted to test and develop RAIM systems. In basic RAIM, it is assumed that more than one faulty satellite does not occur simultaneously. On this basis, if RAIM is available, accuracy requirements can be estimated. The advantage of RAIM is that it does not require additional hardware and is evaluated at the user level [2]. Integrity monitoring at the user level is crucial because it is the only place where all the information necessary to solve navigation problems is applied. System integrity includes the system's ability to issue timely alerts to the user.

This paper tries to detect and mitigate spoofing by introducing an Advanced RAIM (ARAIM) algorithm and removing RAIM limitation of identifying only one faulty satellite. ARAIM supports multi-constellation dual-frequency [3]. In this method, two main topics are generally addressed through two separate tests. The first topic is RAIM availability, which is assessed in the

Iranian Journal of Electrical & Electronic Engineering, 2026.
Paper first received 30 Jul 2025 and accepted 03 Dec 2025.
* The author is with the Department of Advanced Engineering, Faculty of Advanced Technologies, University of Mohaghegh Ardabili, Namin, Iran.
** The author is with the Department of Electrical Engineering, Iran University of Science and Technology Narmak, Tehran 16846-13114, Iran.
*** The author is with Department of Computer Science, Universidad de Valladolid.
E-mails: moazedi@uma.ac.ir, m_mosavi@iust.ac.ir and diego.martin.andres@uva.es.
Corresponding Author: M. Moazedi

position domain, and the second is error detection, which is evaluated in the measurement domain. Initially, we need a closer examination of satellite geometry from the user's perspective to determine whether the current satellite geometry allows the application of the RAIM method. If this condition is met, RAIM is considered available, and in the second step, error detection is conducted. This is meaning that the second test is performed following a positive result from the first. Both of these tests require a threshold for decision-making. This threshold is a key factor linking the two tests. Three different methods are used for the second test: (1) the range comparison, (2) the least squares residual [4], and (3) the parity methods. These are largely equivalent, with key considerations being the definition of the test statistic, the decision threshold, and computational complexity. Here, the least squares residual method is employed.

RAIM algorithm is divided into the snapshot algorithm based on the pseudo-range residual and the algorithm based on the Kalman Filter (KF) [5-7]. As a typical algorithm of snapshot algorithm, parity vector method is simple to calculate and has shown good detection performance for large pseudo-range deviation. And its improved algorithm is sensitive for small and slowly-changing pseudo-range deviation [8]. Compared with the snapshot algorithm, the RAIM algorithm based on Kalman filtering is less sensitive to slow-varying fault detection due to the memory effect of the filter. Nevertheless, it eliminates the limitation imposed by satellite quantity requirements and is capable of performing independent fault detection effectively. For these reasons, this paper adopts the KF-based RAIM algorithm.

The remainder of this paper is organized as follows: Section 2 states literature review. Section 3 reviews basic RAIM application is spoofing mitigation and availability assessment. Section 4 proposes the KF based ARAIM method. Section 5 gives an overview of the simulation results. Section 6 concludes this work with a brief summary.

2 Review of Previous Research

Various RAIM schemes have been proposed, typically based on residual analysis, which is the difference between predicted and actual measurements (Fig. 1) [9]. Error detection can be performed using statistical hypothesis tests. The test statistic parameter, based on the residuals, is calculated and compared with a threshold [10]. An error is confirmed if the test statistic exceeds this threshold. RAIM requires at least one degree of redundancy to detect the presence of an error in the measurement set, and once an error is detected, at least two degrees of redundancy are needed to remove it from the navigation solution. The first RAIM error detection algorithm for GPS use was proposed in the second half of the 1980s, with the Fault Detection and Exclusion (FDE) algorithm introduced in 1990 [11].

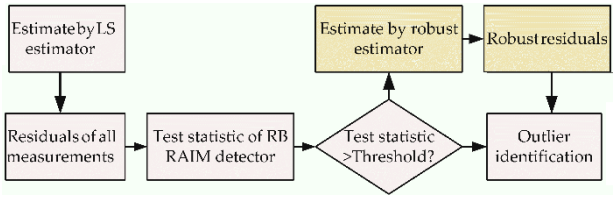


Fig. 1 Flowchart of a residual-based RAIM detector based on a robust estimator [9].

With advances in technology, it has become possible to simultaneously use two or even multiple satellite navigation systems. In this case, RAIM availability increases, but naturally, the number of satellites being tracked for navigation at any given moment also increases. As a result, the likelihood of multiple satellites being faulty rises, making the assumption of only one faulty satellite no longer valid, and the conventional RAIM approach less effective.

Accordingly, various improvements have been proposed for RAIM to handle multiple simultaneous faults, which generally consider the integration of other satellite systems such as Galileo, INS, GLONASS, and Beidou. These methods generally assume that one satellite system may be faulty while another remains fault-free [12–19]. Extensive theoretical and experimental research has been conducted on the testing and development of RAIM systems. RAIM techniques capable of excluding more than one erroneous or spoofed signal require additional information, such as measurements on other frequencies or from other satellite systems, which increases implementation complexity [20].

In recent years, most researchers have focused on ARAIM, in which PL (a threshold for positional error) is calculated after fault detection [21]. Jiang and Wang adopted the ideal PL [22] in ARAIM and verified it was more accurate than other PLs for the ARAIM availability assessment [17]. ARAIM is still in the theoretical research stage and is not currently being applied in engineering practice. In this paper, an ARAIM is proposed and implemented, which analyzes scenarios where two or more spoofed signals are received by the receiver (even under the assumption that the spoofed signals are otherwise identical to valid signals except for their pseudo-range measurements).

3 Implementation of Basic RAIM

Based on the presented concepts, the GPS measurement model is represented as Eq. (1):

$$y = Gx + f \quad (1)$$

where y is the linearized measurement vector (of size N×1), representing the difference between the pseudo-ranges and the calculated ranges based on the positions of the primary satellites (with N being the number of satellites tracked for positioning). x is a 4×1 vector that includes three components of the deviation of the actual position from the assumed position, plus the clock bias deviation. G is the observation matrix or design matrix (of size N×4), which is a linear association matrix based on the linearization around the user's assumed position and clock bias. F is the measurement error vector, encompassing receiver noise, signal propagation effects, ephemeris errors, and other sources of noise [11].

In satellite navigation signal processing, it is generally assumed that G is known. In practice, G contains a set of vectors from the actual user position to the satellite positions. Therefore, this matrix is subject to disturbance associated with ephemeris errors and user position errors. Such discrepancies can affect the detection process, especially in the presence of satellite faults or signal interference. The least squares estimate for X' can be obtained as Eq. (2):

$$x_{LS} = (G^T G)^{-1} G^T . y = A . y_{LS} \quad (A = (G^T G)^{-1} G^T , y_{LS} = G x_{LS}) \quad (2)$$

This estimation provides the solution for the deviations in position and clock bias using the available pseudo-range measurements. The value y_{LS} is an estimate of y and is used in calculating the residual vector. The residual vector, which represents the difference between y and its estimated value, is ultimately obtained from as Eq. (3):

$$\varepsilon_{ls} = y - y_{LS} = [I - G(G^T G)^{-1} G^T](f) = Sf \quad (3)$$

This process is a linear transformation that takes the measurement error and converts it into a residual vector. After obtaining the residual vector, it is used to calculate the Sum of Squared Errors (SSE), which plays a crucial role in the RAIM method.

$$SSE = (f)^T S^2 (f) = \varepsilon_{LS}^T \varepsilon_{LS} \quad (4)$$

The *SSE* parameter as a non-negative quantity, has important properties in the least squares decision-making rule, simplifying the decision process. It is divided into two parts: one for the error-free section and one for the error-containing section, with the decision point called the threshold. The statistical distribution of *SSE* is entirely independent of satellite geometry for any *N*, making it easier to perform the fixed-threshold alert algorithm. The task reduces to calculating thresholds that yield the desired alert rate for varying expected values of *N* [19].

Making a decision to announce an error requires two values: the test statistic parameter and the threshold. Typically, the detection threshold is determined from the statistical properties of the test statistic, ensuring that false alerts—those occurring under error-free conditions—do not exceed a specified rate. Before addressing detection in basic RAIM, we first need to discuss RAIM availability, followed by the detection phase.

3.1 RAIM Availability

For RAIM availability, the geometry of the satellites needs to be evaluated. The first requirement for geometry is that the user must have at least five visible satellites. For each visible satellite, a slope value is calculated, representing the degree of impact that the satellite error has on the user error. To make a conservative estimate, it is assumed that an error occurs in the pseudo-range measurements that has the greatest impact on the navigation solution. This is known as the maximum slope, and using this value ($Slope_{max}$), the PL and AL parameters are calculated. PL is within the safe operation limit AL (the maximum allowable error for safe operations). PL is used to ensure that the error of the method does not exceed a specified amount [5].

The comparison of these two parameters determines the availability of RAIM. In fact, fault detection calculations are performed only if PL ≤ AL. Typically, a distinction is made between the Horizontal PL (HPL) and Vertical PL (VPL). Ultimately, the satellite geometry at the user's position is valid for RAIM error detection if HPL≤ HAL, VPL≤VAL, and n>4.

A numerical search for the ideal PL begins with an improbably large value [23], which leads to a large amount of calculation, increasing the computational burden of a GNSS receiver or an onboard computer. PL depends on the satellite geometry (including the number of visible satellites), minimum detectable bias and statistical assumptions about the measurements. Note that AL is also a fixed value. To calculate PL, we need to calculate the slope parameter, which is defined for both horizontal and vertical protection levels as the ratios of Horizontal Radial Error (HRE) and Vertical Error (VE) to the test statistic, respectively. The following equations relate to determining RAIM availability.

$$Slope_{hi} = \frac{HRE_i}{test\ statistic} \quad (5)$$

$$Slopev_i = \frac{VE_i}{test\ statistic} \quad (6)$$

$$test\ statistic = \sqrt{SSE} \quad (7)$$

$$SSE = (f_i S)^T (f_i S) = f_i^T (S) f_i = {f_i}^2 S_{ii} \quad (8)$$

$$HRE = \sqrt{(A_{11} f_1 + A_{12} f_2 + \cdots + A_{1n} f_n)^2 + (A_{21} f_1 + A_{22} f_2 + \cdots + A_{2n} f_n)^2} = \quad (9)$$

$f\sqrt{A_{1i}^2 + A_{2i}^2}$

$$VE_i = f_i A_{3i} \quad (10)$$

Assuming that only i-th satellite contains an error and other satellites are error-free, the sensitivity of horizontal positioning error to the error in i-th satellite is expressed as Eq. (11):

$$Slope_i = \sqrt{(A_{1i}^2 + A_{2i}^2)/S_{ii}} \quad (11)$$

or

$$Slope_i = \sqrt{(A_{1i}^2 + A_{2i}^2)(N-4)/S_{ii}} \quad (12)$$

where $A_{i,j}$ refers to the element in i-th row and j-th column of matrix A. Diagonal matrix S_{ii} is element of diagonal matrix S. Maximum slope can be determined as Eq. (13):

$$Slope_{max} = \underset{i=1,2,\ldots,n}{Max}\{Slope_i\} \quad (13)$$

A satellite with the largest $Slope_{max}$ is more difficult to detect, as it produces the smallest test statistic for a given positioning error [20]. PL is determined using Eq. (14), where $Pbias$ is equal to the product of the standard deviation and the non-centrality parameter. The non-centrality parameter λ defined as the mean normal of squared measurement residuals with degrees of freedom k:

$$PL = Slope_{max} * Pbias \quad (14)$$

$$P_{bias} = \sigma\sqrt{\lambda} \quad (15)$$

$$\lambda = km^2\ ,\ k = N - 4 \quad (16)$$

After calculating PL and comparing it to AL, RAIM availability is determined, and if the result is positive, the error detection phase is performed [14].

3.2 Spoofing Detection using Basic RAIM

When RAIM is available, the fault detection phase is executed by calculating the test statistic and the threshold parameters. In residual-based RAIM, the test statistic is defined as the weighted norm of the residual vector and is proportional to the positioning error as well as the magnitude of the erroneous component. In general, RAIM algorithms determine the threshold using both Monte-Carlo sampling and the chi-square probability distribution. In this case, the chi-square method is used as Eq. (17):

$$Threshold = F^{-1}_{\chi^2_{N-4}}(1 - P_{FA})\sigma^2 \quad (17)$$

where F is the central chi-square distribution function, P_{FA} is the maximum allowable false alarm rate, and σ is the assumed standard deviation of the measurement error. P_{fa} is also expressed as Eq. (18):

$$P_{FA} = \int_T^{\infty} f(x)dx \quad (18)$$

where $f(x)$ is the probability density function in the fault-free condition. In the literature, P_{FA} is typically considered a fixed value, usually between $7.7 \times 10^{-7}$and 0.001. As previously mentioned, basic RAIM can only exclude one spoofed satellite. RAIM-based FDE is considered available if fault detection remains possible even after exclusion. The exclusion algorithm identifies the satellite causing the fault and removes it from the navigation solution.

In summary, the standard RAIM algorithm for detecting spoofing with a single spoofed satellite is implemented based on the flowchart shown in Fig. 2. This algorithm can provide continuous accuracy monitoring for GPS navigation by analyzing the residual pseudo-ranges.

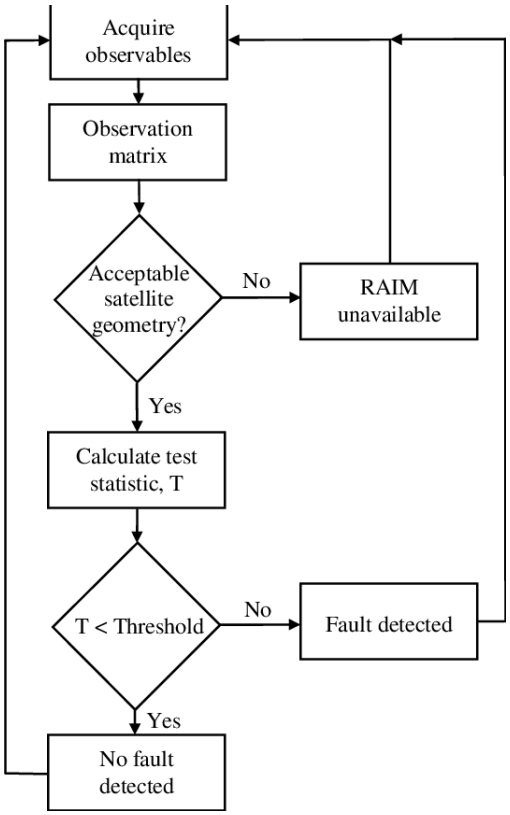


Fig. 2 Baseline RAIM algorithm expanded from Sandstrom 2001 [15].

To identify the spoofed satellite, the exclusion algorithm checks the residual vector after a fault is detected. Based on the discrepancy in the array value associated with the spoofed satellite in the residual vector, it identifies the channel of the spoofed satellite, removes it from the navigation calculations, and then resumes navigation.

4 The Proposed Kalman filter based ARAIM

Compared with ARAIM, the basic RAIM has two deficiencies. The first is that RAIM is designed for a single constellation, monitoring only a single satellite fault [2]. ARAIM is designed for double constellations, monitoring not only the single satellite fault, but also the

multiple satellite faults and the constellation fault [12]. The second is classic, and the enhanced PLs are not rigorous enough for RAIM availability assessment, while the PL of ARAIM is much more rigorous. However, the on-board calculation of RAIM using the classic or the enhanced PLs is much less than that of ARAIM. For a single constellation, RAIM can still be used, but there is a problem needs to be considered, founding a RAIM availability assessment method both satisfying the rigor and maintaining the low on-board computational burden.

In this paper, a slope-based RAIM availability assessment method is proposed to solve the above problem. The characteristic slope is taken as the assessment basis. Using the ideal slope threshold, this method can achieve a consistent RAIM availability assessment with the ideal-PL-based method. The ideal slope threshold can be calculated offline and searched online because it is only related to one geometric parameter.

Besides, Kalman innovation monitoring is used to estimate the current measurement by historical information, comparing with the current actual measurement to determine whether there is a range fault. The fault of each satellite can be independently detected with less computation, fewer stars and multiple faults, overcoming the shortcoming of the snapshot algorithm. But note that KF method is not sensitive to slowly-changing faults, which is mainly due to the fact that the test statistic is not only related to the fault deviation of the current time, but also to the estimated deviation before the current time.

4.1 Difference between Multi-Fault and Single-Fault

The comparison between the test statistic and the threshold is based on the idea that when ‖f‖ (the measurement error vector) increases, ‖y‖ (the residual vector) is also likely to increase. This assumption generally holds true in the case of a single faulty satellite. However, it has been observed that ‖y‖ does not necessarily increase proportionally with ‖f‖. The effect of the error on ‖f‖ is a function of the geometry between the satellite and the receiver and is, in fact, a scalar quantity. Furthermore, it has been observed that RAIM performance is not guaranteed in the presence of multiple faulty satellites. This is because, in the multi-fault case, the individual errors can cancel each other out, and as a result, ‖y‖ might not increase (even when there are significant biases in the ‖f‖ components [16]).

Simulation results show that multiple faults reduce RAIM availability, and methods effective for single-fault cases do not perform well under multiple faults. Some methods have been proposed to improve RAIM availability compared to conventional RAIM, including Novel Integrity- Optimized RAIM (NIO-RAIM), which applies weights to the pseudo-range measurements, but these still operate under the single-fault assumption [8]. Indeed, the core structure of RAIM algorithms remains the same for both single- and multi-fault scenarios. Therefore, using the same pseudo-range error standard deviation and false alarm probability, the decision threshold remains unchanged in both cases. The difference lies in the specific slope values, both horizontal and vertical slopes, which represent the ratio of navigation solution errors to residual distance errors [3]. Thus, in the next section, a method for calculating the maximum slope is proposed to improve the RAIM availability algorithm.

4.2 New method for Generalizing RAIM Availability

Since the key difference between the single-fault and multi-fault cases lies in their specific slope values, the first step in generalizing RAIM for spoofing detection should be to determine the $Slope_{max}$. Following the assessment of RAIM availability, and upon confirmation of a positive outcome, the system proceeds to the fault detection stage. The error vector in the positioning equation is expressed by as Eq. (19):

$$S_{err} = x_{LS} - x = Af \tag{19}$$

This approach emphasizes calculating $Slope_{max}$ to understand the worst-case effect a spoofed or faulty satellite can have on the navigation solution. With that, the RAIM algorithm can be generalized to consider multiple faults more robustly. Assuming that faults have occurred in satellites *i*, *j*, and *k*, the error vector can be represented as Eq. (20):

$$\begin{aligned} &e = f_i \cdot g_i + f_j \cdot g_j + f_k \cdot g_k \ , \\ &f = (0, \dots, b^{(i)}, 0, \dots, 0, b^{(j)}, 0, \dots, 0, \dots, b^{(k)})^T \end{aligned} \tag{20}$$

where f_i, f_j, f_k are the magnitudes of the errors in the pseudo-range measurements from satellites *i*, *j*, and *k*, respectively. g_i, g_j, g_k are the corresponding direction vectors (or columns of the geometry matrix G) that relate measurement errors to position domain errors. Based on the two preceding equations, the error vector can be rewritten as Eq. (21). For horizontal error, the north and east components of the position error vector are considered. Also, for vertical error, the west component is taken into account. These errors are derived from equations (22) and (23). Based on advance VE and HRE, the new equations on SEE and slope can be updated as equations (24) and (26).

$$S_{err} = Af = [b^{(i)}A_{1i} + b^{(j)}A_{1j} + b^{(k)}A_{1k}, b^{(i)}A_{2i} + b^{(j)}A_{2j} + b^{(k)}A_{2k}, b^{(i)}A_{3i} + b^{(j)}A_{3j} + b^{(k)}A_{3k}, b^{(i)}A_{4i} + b^{(j)}A_{4j} + b^{(k)}A_{4k}] \tag{21}$$

$$VE = \left| b^{(i)} A_{3i} + b^{(j)} A_{3j} + b^{(k)} A_{3k} \right| \tag{22}$$

$$HRE = \sqrt{(b^{(i)} A_{1i} + b^{(j)} A_{1j} + b^{(k)} A_{1k})^2 + (b^{(i)} A_{2i} + b^{(j)} A_{2j} + b^{(k)} A_{2k})^2} \tag{23}$$

$$SSE = \varepsilon_{LS}^T \varepsilon_{LS} = f^T(S) f = (b^{(i)})^2 S_{ii} + (b^{(j)})^2 S_{jj} + (b^{(k)})^2 S_{kk} + 2b^{(i)} b^{(j)} S_{ij} + 2b^{(i)} b^{(k)} S_{ik} + 2b^{(k)} b^{(j)} S_{kj} \tag{24}$$

$$Slope_V^{(i,j)} = \frac{VE}{\sqrt{SSE}} = \frac{\left| b^{(i)} A_{3i} + b^{(j)} A_{3j} + b^{(k)} A_{3k} \right|}{(b^{(i)})^2 S_{ii} + (b^{(j)})^2 S_{jj} + (b^{(k)})^2 S_{kk} + 2b^{(i)} b^{(j)} S_{ij} + 2b^{(i)} b^{(k)} S_{ik} + 2b^{(k)} b^{(j)} S_{kj}} \tag{25}$$

$$Slope_V^{(i,j)} = \frac{HRE}{\sqrt{SSE}} = \sqrt{\frac{(b^{(i)} A_{1i} + b^{(j)} A_{1j} + b^{(k)} A_{1k})^2 + (b^{(i)} A_{2i} + b^{(j)} A_{2j} + b^{(k)} A_{2k})^2}{(b^{(i)})^2 S_{ii} + (b^{(j)})^2 S_{jj} + (b^{(k)})^2 S_{kk} + 2b^{(i)} b^{(j)} S_{ij} + 2b^{(i)} b^{(k)} S_{ik} + 2b^{(k)} b^{(j)} S_{kj}}} \tag{26}$$

These relations also cover one or two spoofed satellites, and are capable of identifying up to three spoofed satellites. In fact, by calculating $Slope_{max}$ using the above equations, the value of PL is obtained and the RAIM availability is determined. Simulation results show that the ARAIM is a viable approach for detecting and eliminating two or more spoofing signals.

4.3 ARAIM algorithm Using Kalman Filter

In the case where multiple spoofed satellites are present, removing the channels related to the spoofed satellites or pseudo-ranges is only possible if the number of spoofed pseudo-ranges is known. The spoofing mitigation approach proposed in this study proceeds as follows: navigation is maintained using the best subset, defined as the group of at least four satellites that produces the minimum test statistic, as determined by the algorithm. It is important to emphasize that the test statistic for each subset is computed using Eq. (7). Although navigation with the best subset may still contain a spoofed pseudo-range, the KF is subsequently employed to estimate the spoofed pseudo-range and thereby enhance navigation accuracy. The KF is a set of equations and mathematical relations that functions as an optimal estimator with prediction and correction capabilities by minimizing the error covariance. This filter enables estimation for past, present, and future states. Even when the exact nature of the modeled system is unknown, the KF can still perform these calculations. In this filter, the state of the stochastic process to be estimated is expressed through equations (27) and (28).

$$x_k = Ax_{k-1} + w_{k-1} \tag{27}$$

$$z_k = HX_k + v_k \tag{28}$$

The variables w_{k-1} and v_k represent the measurement and process noises and are considered as mutually independent white noise processes with normal distribution. In these equations, x_k is the state vector of the process at time t_k. A is the transition matrix from x_{k-1} to x_k. Note that in practice, A may vary over time, but here it is assumed to be constant. z_k is the measurement vector at time t_k. H is the ideal observation matrix that relates the measurement vector to the state vector at time t_k, which may also vary with time or measurements in practice; however, it is considered constant in this case. The system error is expressed as Eq. (29):

$$e_k^- \equiv x_k - \hat{x}_k^-$$
$$e_k \equiv x_k - \hat{x}_k \tag{29}$$

where $e_k$represents a priori error estimate, and x_k denotes the best a priori estimate for obtaining a measurement at time t_k, and e_k^- is the updated error estimate. The error covariance matrix at this time is defined as Eq. (30):

$$\bar{P}_k = E[\, \bar{e}_k \bar{e}_k{}^T] \tag{30}$$

where E represents the expected value. Now, the linear combination of the two estimated and measured states is expressed as Eq. (31):

$$\hat{x}_k = \hat{x} + K(z_k - H\hat{x}_k^-) \tag{31}$$

where $\hat{x}_k$represents the next state estimate, z_k denotes the measured value, and *K* is the Kalman gain, which is the weight that minimizes the error between the measured value and the best estimate, and it changes over time. In Eq. (32), the updated error covariance is provided. After some mathematical calculations, the error covariance matrix is expressed in Eq. (33) which is a general expression for updating the error covariance matrix and is used for any value of *K*. Therefore, the gain K_k is calculated from Eq. (34):

$$\bar{P}_k = E[e_k e_k^T] = \mathrm{E}[(x_k - \hat{x}_k)(x_k - \hat{x}_k)^T] \tag{32}$$

$$P_k = (I - K_k H_k)\bar{P}_k (I - K_k H_k)^T + K_k R_k K_k{}^T \tag{33}$$

$$K_k = \bar{P}_k H^T (H\bar{P}_k H^T + R)^{-1} \tag{34}$$

Based on the above relations, the KF estimates a process using feedback control. The filter predicts the process state at a given time and then receives feedback in the form of a noisy measurement. This is why the KF equations are divided into two categories: (1) time update equations and (2) measurement update equations. The first are responsible for predicting the current state and estimating the error covariance to obtain the prior

state for the next time step. The second are responsible for applying the feedback.

The time update equations can also be considered as predictor equations. In contrast, the measurement update equations are considered as corrector equations. It is clear that the final estimation algorithm is a prediction-correction algorithm for solving numerical problems.

The Kalman algorithm is applied in the following order: The first step in the measurement update process is to calculate the Kalman gain K_k. The next step is the updated estimation with the measurement vector z_k. The third step is to compute the error covariance for the updated estimation using relation, and the fourth step is a forward propagation step using relations, which are essentially the prediction equations. Figure 3 provides a general overview of the filter's performance, integrating the high-level diagram with the time update relations and measurement update. In the proposed algorithm, by defining a threshold, the pseudo-range falsification is first detected, and then, based on the overall KF process, the data is fed into the filter. The proposed ARAIM algorithm with KF estimator is generally implemented based on Fig 4.

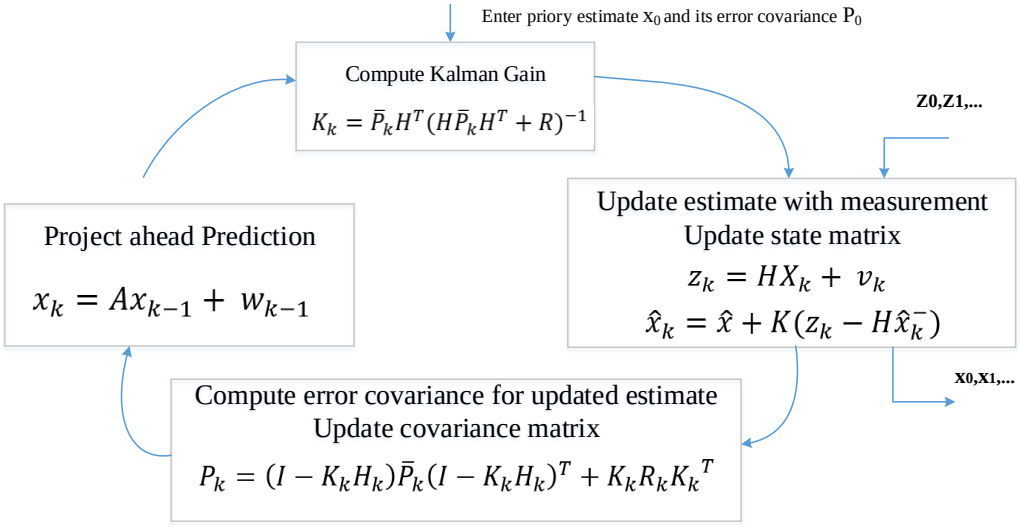


Fig. 3 General overview of the Kalman filter.

5 Simulation Results

The results of the simulation for 8 datasets are presented in this section. All datasets employed in this study correspond to a medium level of GPS spoofing and were generated using a combination of authentic GPS data and a GPS signal simulator. Specifically, a genuine static GPS signal was superimposed with its time-delayed replicas at varying intervals. A comprehensive description of the dataset generation process is provided in Ref. [13], previously published by the authors. All processing was done on a laptop ASUSK46C with i5 1.8 GHz CPU.

Before the results will entail, the satellite acquisition results for dataset1 are displayed in the valid and spoofing signal sections in Fig. 5.

As can be seen, after the spoofing is applied, the satellite acquisition level changes and a spoofed satellite is added. As discussed previously, the spoofing affects the pseudo-range between the satellite and the receiver, and this effect can be observed in Fig. 6. Table 1 presents the residual vector values for each satellite. In the presence of spoofing, the norm of the residual vector increases, which affects the sum of the squared errors and, consequently, the corresponding statistic.

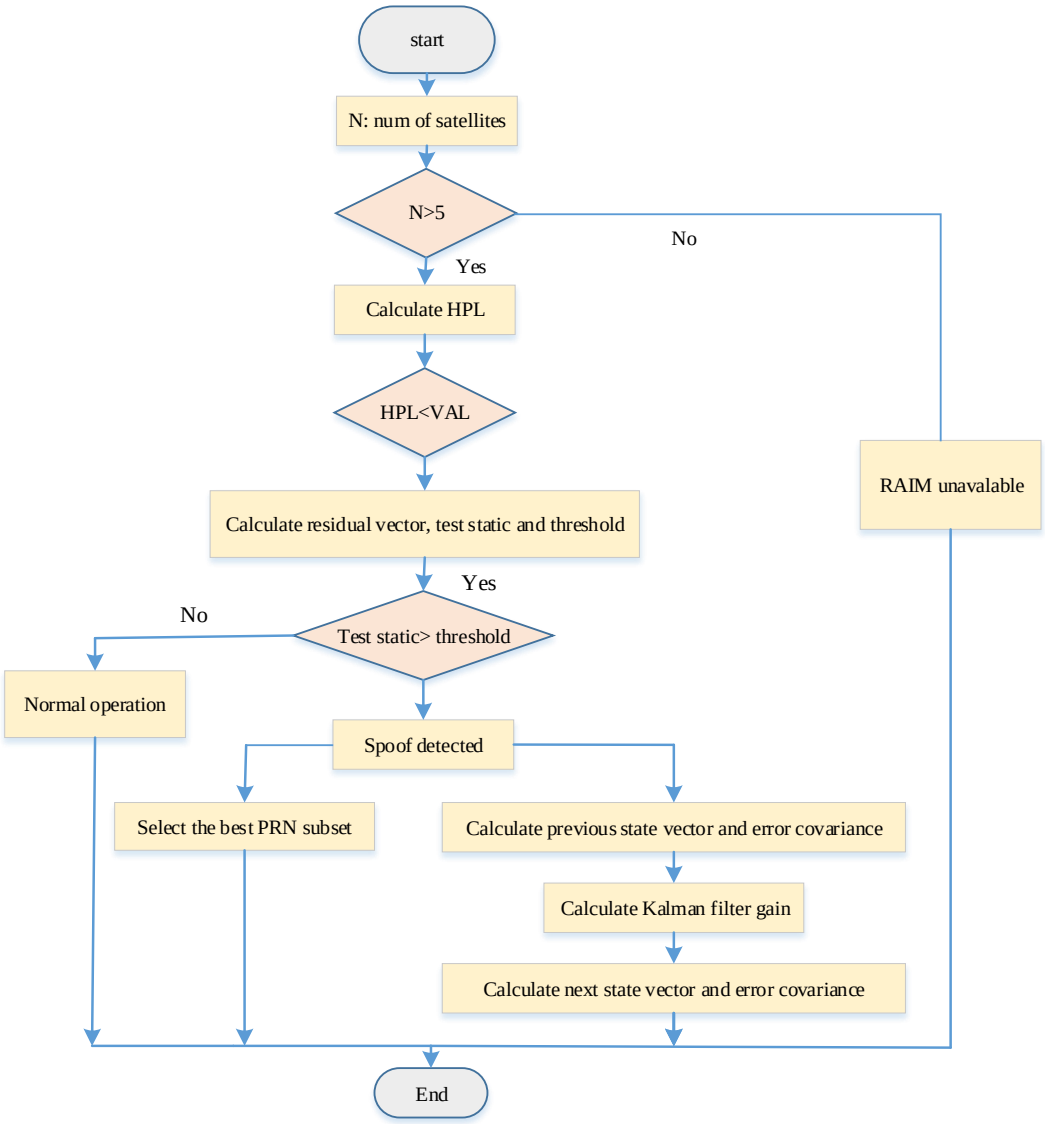


Fig. 4 Flowchart of the proposed ARAIM anti-spoofing algorithm based on Kalman filter

Table 1. The residual vector values for each satellite in data set1.

Authentic		Spoofing	
PRN No.	Residual vector	PRN No.	Residual vector
3	-6.647318017	19	-13.23528333
13	-3.19119784561	22	5.15325278
14	-0.776807732	3	-1.50101150
22	-0.249262851	6	-13.83188533
6	4.482189685	18	23.41492799
norm	8.66753521	norm	30.71744932

5.1 Spoofing Mitigation in Basic RAIM

In Table 2, the results related to the accessibility test in the base RAIM are presented. Dataset2 to dataset4 are similar to dataset1 have one fake PRN. The slope values are stated separately for both horizontal and vertical directions. As previously mentioned, the warning threshold value is considered constant, which is 40 meters for the horizontal threshold and 50 meters for the vertical threshold, respectively [8].

Based on the obtained values for all data sets, the result of the accessibility test is positive. Table 3 shows the values of the test statistic for the error detection stage. The parameters considered for this stage are $P_{fa} = 0.00055$, $\sigma = 4$ and $threshold = 13.82057$. Since all

four datasets track 5 satellites, they have a Degrees of Freedom (DOF) of 1, and the threshold value for all four datasets is the same. Based on the observed results, the basic RAIM successfully detects the deception in the presence of one fake satellite. Based on the values of the residual vectors, the algorithm identifies the fake satellite and removes it from the navigation. The results of the RMS error value in the presence of deception and after its reduction are shown in Table 4. During various tests, we were able to reduce more than 53% of the deception.

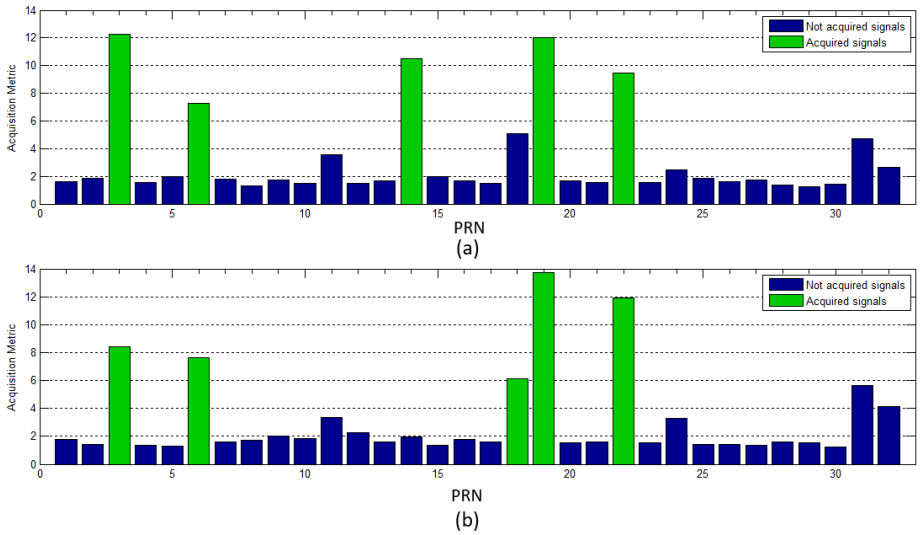


Fig. 5. Acquisition results of dataset1: (a) authentic and (b) spoofing.

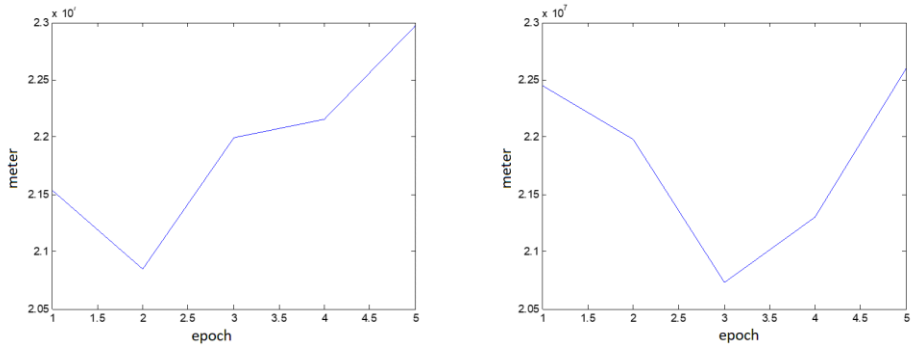


Fig. 6 Pseudo-range values of dataset1: (a) authentic and (b) spoofing.

Table 2. Accessibility test results for all dataset1to dataset4.

Data set	*Pbias*	$slope_{max}^{H}$	*HPL*	$slope_{max}^{V}$	*VPL*
1	2.47360731	18.68072575	46.20877977	19.50955894	48.25898761
2	3.59490513	5.70003795	18.22618269	3.16506199	11.37809762
3	1.64611265	9.89939901	16.46112650	3.47310345	5.71711953
4	2.10478901	6.32139994	13.30521317	3.97179223	8.35978494

5.2 Spoofing Mitigation with Kalman filter RAIM

In this section, 4 datasets with 2 or 3 fake PRN are utilize for ARAIM algorithm evaluation. First, the acquisition results and the values of the pseudo-range for the spoofing and authentic signals are visible in Figures 7 to 14. For each dataset, the residual vector values after simulation are provided in Tables 5 to 8.

The result of the access test simulation in the generalized case is shown in Table 9. The access test result, by comparing the values of the PL and the threshold warning level in both horizontal and vertical modes, is positive.

Table 3. Test statistic for authentic and spoofing.

Data set	Number of satellites		Test statistic	
	(spoof) N_S	(authentic) N_A	(S)	(A)
1	5	5	14.12	13.8105
2	5	5	13.93	13.1904
3	5	5	16.06	13.205
4	5	5	19.066	13.274

Table 4. Spoofing reduction in basic RAIM.

Data set	RMS (before)[m]	RMS (after) [m]	Reduction [%]
1	52.66	13.94	73.52
2	59.57	18.53	68.89
3	79.11	21.87	72.35
4	36.9	17.19	53.41

Table 5 Residual vector for each satellite in dataset5.

PRN number in spoofing data	Residual vector value
31	-1.31115748
32	-0.22441087
13	-6.00720883
23	2.24841350
20	5.07436373

Table 6 Residual vector for each satellite in dataset6.

PRN number in spoofing data	Residual vector value
31	3.12309706
32	-2.16323653
23	9.00867440
13	-18.32675761
11	-16.01573932
20	24.37396196
1	10.36878861

Table 7 Residual vector for each satellite in dataset7.

PRN number in spoofing data	Residual vector value
31	4.59252516
23	5.67678309
1	-10.91725037
20	13.89320010
13	3.98320010
11	11.55771318

Table 8 Residual vector for each satellite in dataset8.

PRN number in spoofing data	Residual vector value
23	-10.88896569
1	-11.175233729
31	-7.08271553
20	21.02701308
11	-14.23056913

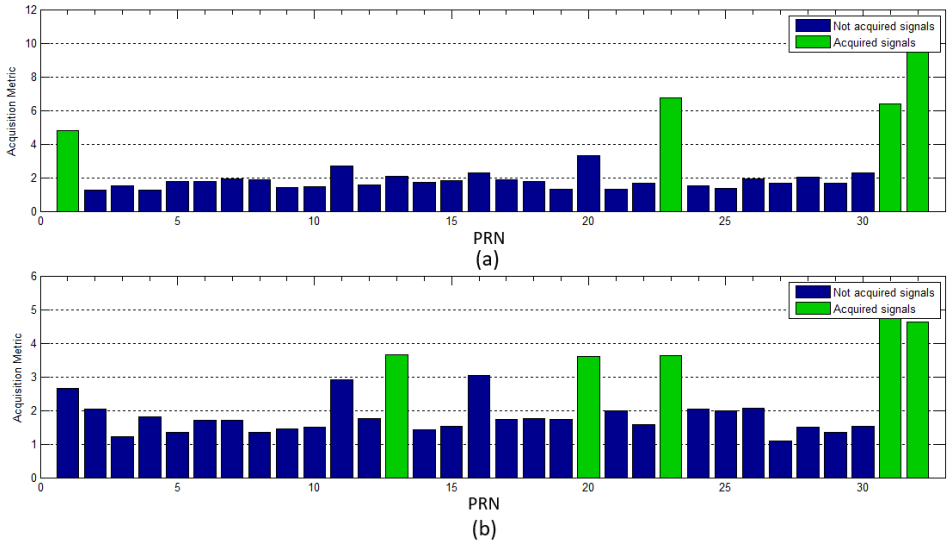


Fig. 7 Acquisition results of dataset5: (a) authentic and (b) spoofing.

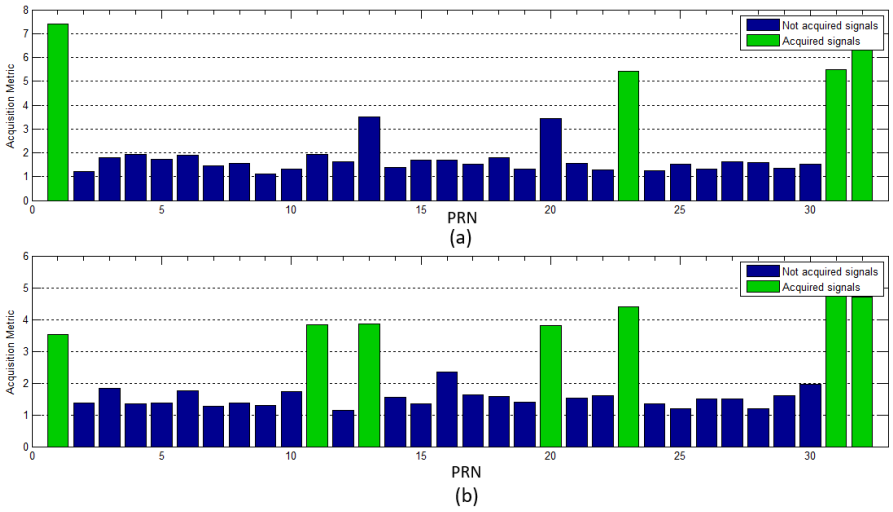


Fig. 8 Acquisition results of dataset6: (a) authentic and (b) spoofing.

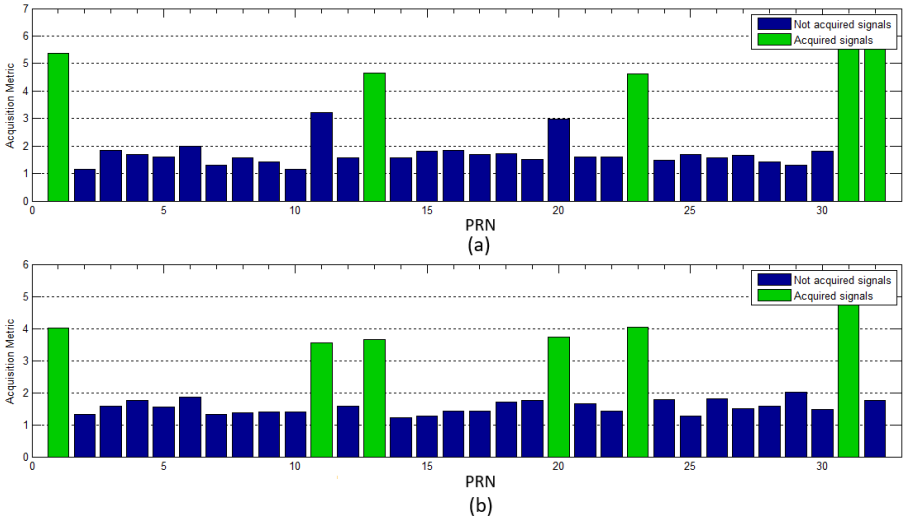


Fig. 9 Acquisition results of dataset7: (a) authentic and (b) spoofing.

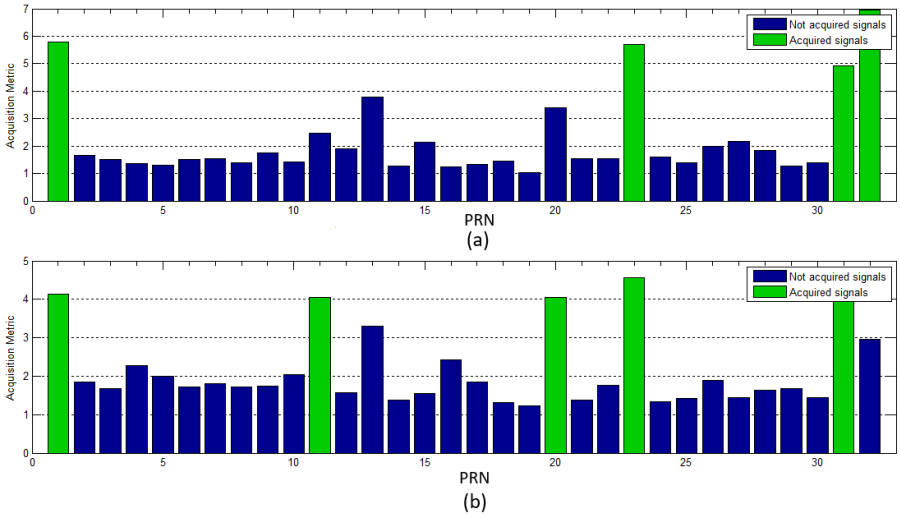
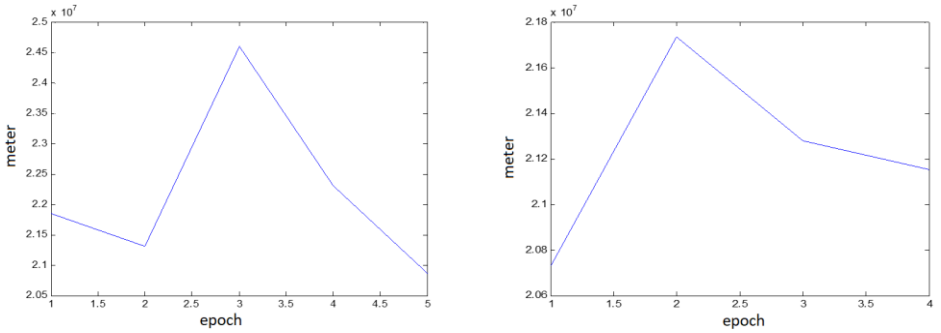
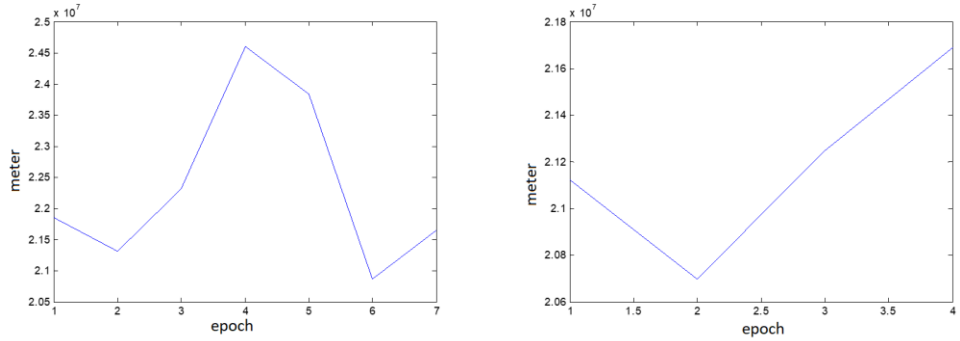


Fig. 10 Acquisition results of dataset8: (a) authentic and (b) spoofing.



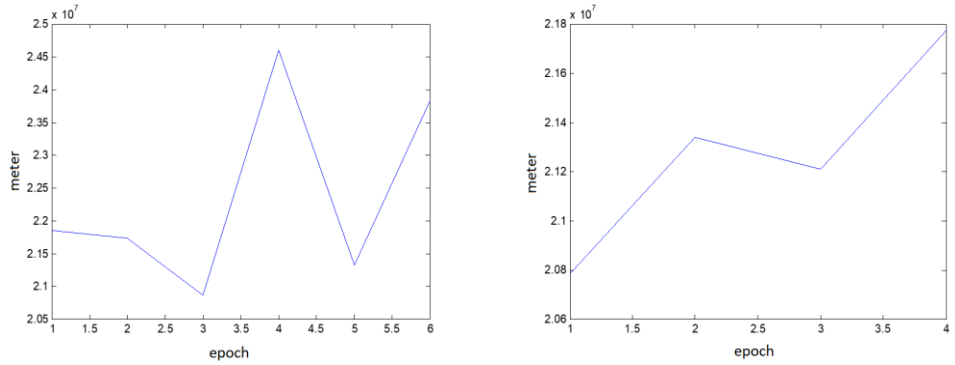
(a) (b)

Fig. 11. Pseudo-range values of dataset5: (a) authentic and (b) spoofing.



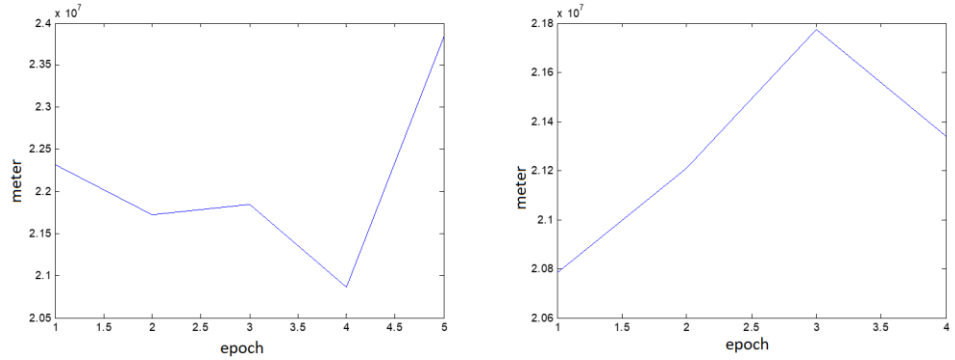
(a) (b)

Fig. 12 Pseudo-range values of dataset6: (a) authentic and (b) spoofing.



(a) (b)

Fig. 13 Pseudo-range values of dataset7: (a) authentic and (b) spoofing.



(a) (b)

Fig. 14 Pseudo-range values of dataset8: (a) authentic and (b) spoofing.

Table 9 Accessibility test results for all datasets 5 to 8.

Dataset	N_S	Num. of fake PRNs	P_{bias}	$slope_{max}^{V}$	VPL	$slope_{max}^{H}$	HPL
5	5	2	39.44045010	5.03398712	47.63678701	6.08012768	7.83483333
6	7	3	13.40043724	3.52229077	26.43692568	7.06095623	3.74409992
7	6	2	10.75976858	1.79119429	48.43939083	8.06378292	6.00703060
8	5	2	24.04690568	3.51294807	45.99047171	7.29153089	6.30738213

Therefore, after that, we executed the error detection stage, and its result is presented in Table 10. As can be seen, test static for smaller Ns is bigger. The details of applying the fraud reduction algorithm with the KF are shown in Table 11. This algorithm was also able to reduce fraud by more than 64%. Finally, Table 12 presents a comparison of the overall performance of the proposed method against three reference approaches. The comparison is organized into three columns, reporting the average runtime, the achieved spoof reduction, and the resulting Figure of Merit (FOM), which is calculated as the ratio of the normalized reduction to the runtime.

Table 10 Test results of ARAIM for spoofing datasets 5 to 8.

Dataset	N_S	DOF	Test static	threshold
5	5	1	14.33649918	13.82057617
6	7	4	11.02789369	11.02789369
7	6	6	13.6269345	12.86270128
8	5	1	15.93367087 1	13.82057617

Table 11 Spoofing reduction by proposed ARAIM.

Dataset	PRN set	RMS (Before) (meter)	RMS (After) (meter)	Reduction (%)
5	31-32-13-23	177.46	51.25	71.12
6	31-32-23-11	170.34	65.47	61.56
7	31-1-13-11	216.72	70.80	67.33
8	23-1-31-20	243.52	58.15	76.12

Table 12 comparison the proposed ARAIM with others.

Method	Run time (sec)	Reduction (%)	FOM
[17]	7.5	71	0.52
[19]	2.9	54	1
[20]	11	72	0.36
This work	3.3	69	1.16

6 Conclusion

In this paper a new ARAIM method with KF was proposed, building upon previous works of the authors. The complete details of the fraud process were presented in the tables and figures. The results showed that ARAIM can detect errors in measurements in spoofing attacks with more than one fake PRN. Moreover, by analyzing the residuals of pseudo-ranges, compensate for the effects of fraud interference and errors caused by fraud attacks on the GPS. To make the most of RAIM's performance, a KF was applied to estimate the fake pseudo-ranges, thus enhancing RAIM's performance. Therefore, detecting and mitigation of spoofing attacks with 2 or more than 2 fake satellites in more than 64% can be achieved. Increasing reduction present will be noticed in future works.

Author Contributions

M. Moazedi: Conceptualization, Methodology, Software Development, Data Curation, Visualization, Investigation, and Writing – Original Draft.

M. R. Mosavi: Supervision, Investigation, and Writing – Review & Editing.

D. Martin: Investigation, and Writing – Review & Editing.

Funding

No funding was received for this work.

Informed Consent Statement

Not applicable.

References

[1] DoD U., DHS U. and DoT U., F*ederal radio navigation plan*, Tech. rep., DOTTSC- RSPA-84.8. 2012.

[2] Kaplan E.D. and Hegarty C. J., *Understanding GPS: principles and applications*, Artech House: Norwood, MA, USA, 2005.

[3] Andres S. and Daniel C., Integrity monitoring applied to the reception of GNSS signals in urban environments, Ph.D. Thesis. 2012.

[4] K. Zarrinnegar, N. Rahemi, and M. R. Mosavi, "A New Stochastic Model to Improve Positioning Accuracy of the Recursive Least Squares Method", Iranian Journal of Electrical and Electronic Engineering, Vol.21, No.3, pp.1-9, 2025.

[5] GPS-Galileo Working Group C ARAIM Technical Subgroup Interim Report. Available online (accessed on 14 April 2024).

[6] Martini I., Rippl, M. and Meurer M., "Advanced RAIM architecture design and user algorithm performance in a real GPS, GLONASS and Galileo scenario", The 26th International Technical Meeting of the Satellite Division of the Institute of Navigation, pp.2624-2636, 2013.

[7] Blanch J., Walter T., Enge P., Wallner S., Amarillo Fernandez F., Dellago R., Ioannides R., Fernandez Hernandez I., Belabbas B., Spletter A., Rippl M., "Critical elements for a multi-constellation advanced RAIM", Navigation, Vol.60, No.1, pp.53–69, 2013.

[8] Hwang Y. and Brown, R. "RAIM-FDE revisited: A new breakthrough in availability performance with NIORAIM", Navigation, Vol.53, pp.41–52, 2006.

[9] Dan S., Chuang S., Zhipeng W., Cheng W., Guifei J., "Correlation-weighted least squares residual algorithm for RAIM", Chin. J. Aeronaut., Vol.33, pp.1505–1516, 2020.

[10] Tran, H. T., Lo Presti L.," Demonstration of Multi-GNSS Advanced RAIM Algorithm using GPS and Galileo Signals", International Conference on Space, Aeronautical and Navigational Electronics, Vol. 113, No. 335, pp.191–196, 2013.

[11] El-Mowafy A., Arora B. S., "The Current ARAIM Availability According to LPV-200 Using GPS and BeiDou in Western Australia", IGNSS 2013 Symposium- The International Global Navigation Systems Society, pp. 1–16, 2013.

[12] Mei H., Zhan X., Zhang X., "GNSS vulnerability assessment method based on ARAIM user algorithm", Forum on Cooperative Positioning 330 and Service, pp.111–115, 2017.

[13] Baziar A.R., Moazedi M., & Mosavi M.R. "Analysis of single frequency GPS receiver under delay and combining spoofing algorithm", Wireless personal communications, Vol. 83, No. 3, pp.1955-1970, 2015.

[14] Crespillo O.G., Langel S.; Joerger M. "Tight bounds for uncertain time-correlated errors with gauss-Markov structure in Kalman filtering", IEEE Trans. Aerosp. Electron. Syst.", Vol.59, pp.347–4362, 2023.

[15] Anon.: *Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System Technology Report*, JohnA. Volpe National Transportation Systems Center, 2001.

[16] Gao Y., Jiang Y., Gao Y. and Huang, G. "A linear Kalman filter-based integrity monitoring considering colored measurement noise", GPS Solutions, Vol. 25, pp.1–13, 2021.

[17] Zhang H., and Jiang, Y. "Overbounding the model uncertainty for Kalman filter-based advanced receiver autonomous integrity monitoring in the presence of time correlation by the hybrid evolutionary algorithm", Electronics, Vol.13, No.22, pp.4384, 2024.

[18] M. Moazedi and M. R. Mosavi, "Anti-Spoofing by Smart Acquisition in Cold-Start with Multiple Hypothesis using Wavelet Transform in a Software GPS Receiver", International Journal of Nonlinear Analysis and Applications, Vol.16, No.1, pp.147-161, 2024.

[19] Jia M., and Kassas Z. M., "Kalman filter-based integrity monitoring for GNSS and 5G signals of opportunity integrated navigation", IFAC-Papers on Line, Vol.55, No.24, pp.273-278., 2022.

[20] Zhao J., Song D. and Wang, J. "An Improved RAIM availability assessment method based on the characteristic slope", Sensors, Vol.24, No.11, p.3283, 2024.

[21] Wang, W., & Xu, Y. "A modified residual-based RAIM algorithm for multiple outliers based on a robust MM estimation", Sensors, Vol.20, No.18, p.5407, 2020.

[22] Shokri Sh., Rahemi N. and Mosavi M. R., "Improving GPS positioning accuracy using weighted Kalman filter and variance estimation methods", CEAS Aeronautical Journal, Vol.11, pp.515-527, 2020.

[23] Bai S., Zhang Y., Jiang Y., Sun W. and Shao W. "Modified two-dimensional coverage analysis method considering various perturbations", IEEE Trans. Aerosp. Electron. Syst., Vol.60, pp.2763–2777, 2024.

Biographies

Maryam Moazedi received her BSc, MSc, and PhD from Iran University of Science and Technology (IUST), Tehran, Iran in 2008, 2011, and 2018, respectively. Now, she is faculty member of Advanced Engineering Department in University of Mohaghegh Ardabili. Her research interests in the area of analog and mixed signal integrated circuits and navigation signal processing.

M. R. Mosavi received his B.Sc., M.Sc., 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 a faculty member (Full Professor) of the Department of Electrical Engineering of IUST. He is the author of more than 600 scientific publications in journals and international conferences in addition to 15 academic books. His research interests include

circuits and systems design. He is also editor in-chief of "Iranian Journal of Marine Technology" and editorial board member of "Iranian Journal of Electrical and Electronic Engineering" and "GPS Solutions".

Diego Martín De Andrés received the B.Sc. degree in computer engineering and the M.Sc. degree in computer science from the Department of Informatics, Carlos III University of Madrid, Spain, where he received his Ph.D. degree in 2012. Now, he is a professor at the Computer Science Department Escuela de Ingeniería Informática de Segovia, Universidad de Valladolid. His main research subjects are internet of things, cyber-physical systems, physically unclonable functions, blockchain, knowledge management, information retrieval, and research methods.