IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 19, 2021, accepted March 1, 2021, date of publication March 8, 2021, date of current version April 8, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3064383

Navigation in GPS Spoofed Environment Using M-Best Positioning Algorithm and Data Association

BETHI PARDHASARADHI, (Member, IEEE), PATHIPATI SRIHARI, (Senior Member, IEEE), AND P. APARNA, (Senior Member, IEEE)

Electronics and Communication Department, National Institute of Technology Karnataka, Surathkal, Surathkal 575025, India

Corresponding author: Pathipati Srihari (srihari@nitk.edu.in)

ABSTRACT Intentionally misguiding a global positioning system (GPS) receiver has become a potential threat to almost all civilian GPS receivers in recent years. GPS spoofing is among the types of intentional interference, in which a spoofing device transmits spoofed signals towards the GPS receiver to alter the GPS positioning information. This paper presents a robust positioning algorithm, followed by a track filter, to mitigate the effects of spoofing. It is proposed to accept the authentic GPS signals and spoofed GPS signals into the positioning algorithm and perform the robust positioning with all possible combinations of authentic and spoofed pseudorange measurements. The pseudorange positioning algorithm is accomplished using an iterative least squares (ILS). Further, to efficiently represent the robust algorithm, the M-best position algorithm is proposed, in which a likelihood-based cost function optimizes the positions and only provides M-best positions at a given epoch. However, during robust positioning, the positions evolved due to spoofed pseudorange measurements are removed to overcome GPS spoofing. In order to remove the fake positions being evolved owing to wrong measurement associations in the ILS, a gating technique is applied within the Kalman filter (KF) framework. The navigation filter is a three-dimensional KF with a constant velocity (CV) model, all the position estimates evolved at a specific epoch are observations. Besides, to enhance this technique's performance, the track to position association is performed by using two data association algorithms: nearest neighbor (NN) and probabilistic data association (PDA). Simulations are carried out for GPS receiver positioning by injecting different combinations of spoofed signals into the receiver. The proposed algorithm's efficiency is given by a success rate metric (defined as the navigation track to follow the true trajectory rather than spoofing trajectory) and position root mean square error (PRMSE).

INDEX TERMS Anti-spoofing, data association, GPS spoofing, M-best positioning, navigation filter, robust positioning, spoofing mitigation.

I. INTRODUCTION

Global navigation satellite system (GNSS) is generally used for providing the position, navigation, and time (PNT) for many civilian and military applications. GNSS, such as GPS, Galileo, GLONASS, BeiDou, NavIC uses a receiver to receive the signals transmitted by the satellites. The received signals are processed to provide the receiver's position with an accuracy of a few meters [1]. Most of the autonomous vehicles rely on GPS, an inertial navigation system (INS), external sensors like radar, lidar, and camera for accurate positioning and navigation [2]. The un-intentional degradation of positional accuracy in GPS is due to multi-path, weak signals, urban environment, indoor environment [3]. However, the recent advancements, in radio frequency (RF) generation, result in the simulation of various types of RF signals with inexpensive devices [4]. Hence, intentionally jamming a GPS receiver or adegradation of positional accuracy or false positioning is possible with the transmission of false GPS like signals [5]. Spoofing is a process of transmitting mimic GPS signals either by using a simulator or a repeater with boosted power. Those fake signals are locked onto the receiver and produces false positioning and results in degraded autonomous navigation for vehicles.

The associate editor coordinating the review of this manuscript and approving it for publication was Laxmisha Rai.

One of the fastest-growing industries throughout the world is autonomous vehicular technology. The primary motivation of this development is to provide assistance to drivers, decrease the number of accidents, and autonomous driving [6]. GPS is an integral part of most of the autonomous vehicular designs for accurate navigation [7]. The misleading of GPS positioning, using false (spoofed) measurements, leads to either degradation in its autonomous navigation performance or threat to the vehicle. The development of novel and efficient spoofing detection and mitigation algorithms is a major requirement for the successful deployment of autonomous vehicular technology. The anti-spoofing techniques for GPS receivers, proposed to date have been reviewed in [5], [8]–[10]. Spoofing attack detection is achieved by trusted reference signals, monitoring the power of the individual signals, calculating the average power of received signals, checking the clock, estimating the bias, considering code and phase consistency rate which has been reported from [11]–[14]. Here, trusting a reference signal includes the availability of software-defined signals, which can simulate the target's trajectories, based on prior knowledge. In a recent communication, the automatic gain control (AGC) and monitoring auto-correlation based method to detect spoofing are proposed in [15] (with an assumption that spoofing signals have higher power than legitimate GPS signals). The signal monitoring techniques demand the receiver's re-design, as these detection algorithms are based upon the internal signal measurements available outside the receiver. One can apply these signal processing techniques, to autonomous navigation of vehicles, to detect the spoofing attack, however, they are unable to diminish the spoofing effects. Therefore, deployment of mitigating methods for spoofing consequences and securing the navigation track is a significant consideration in the civilian GPS receiver design.

The optimal way to counter spoofing threats is by the deployment of authentication techniques, which can effectively combat this intentional interference. In [16], a cryptographic authentication is employed to counter spoofing signals. Additionally, cryptographic based encoding and decoding have been successfully employed to prohibit potential hacking of autonomous vehicles and is presented in [17], [18]. It is expensive to deploy these cryptographic based methods in the GPS receiver design, and to integrate them into relatively inexpensive and widespread civilian GPS receivers. Besides these techniques, there are spatial processing and navigation track-based anti-spoofing techniques [19]. The spatial processing techniques include the direction of arrival (DOA) discrimination, using multiple antennas, by applying spatial diversity [20]. Further, in [21], the exchange of measured GPS code based pseudoranges with neighboring vehicles (by using dedicated short-range communications) has been suggested to safeguard the vehicle from spoofing. In addition, the inertial sensor-based anti-spoofing techniques are proposed in [22]. The range sensors, bearing sensors, and vision sensors are integrated to generate efficient anti-spoofing algorithms and are introduced in [23]. Furthermore, the unknown sudden changes in system state variables are addressed in [24]. Managing the simultaneous localization and mapping (SLAM) and sensor fusion capabilities are presented in [25]. The information of each vehicle's position and their relative distances are incorporated to effectively counter the spoofing and achieving the desired group performance has been suggested in [26].

Recently, a significant portion of the GPS market has been occupied by hand-held devices, emphasizing fast acquisition and reliable positioning, over accurate positioning. Examples like positioning in an urban environment using ill-conditioned GPS, positioning in dense forest, and indoor localization are the problems investigated from [27], [28], and [29] respectively. The least-squares (LS) solution is widely used in GNSS positioning. In such cases, LS gives a reasonable solution, by minimizing the sum of squares of the errors between measurements and the estimated model [1]. On the other hand, another segment of the GPS market is looking for quick navigation solutions on time, than possessing only positional accuracy. For example, a scenario may be considered in which navigation solution's integrity is crucial (autonomous vehicles, surveillance drones, and mobiles). In such instances, a Kalman filtering (KF) based techniques are generally applied to establish navigation over the dynamic trajectory of the target [30].

In all the above contributions of autonomous vehicle positioning in GPS spoofing environment [17], [21], [24]–[26], either authentication of signals or communication among the vehicles is applied to either detect the spoofing or secure the navigation track. Further, multiple vehicles and communications among them are seldom present in practical situations. Moreover, huge buildings and other man-made structures in the urban environment may create low observability of satellites. The majority of contributions reviewed so far reveal that most of the spoofing literature focus on detecting a spoofing attack. Since alleviating measures of this spoofing effect has been scarcely addressed in recent contributions, there is a need to develop mitigating methods with equal importance to GPS receiver design. Accordingly, the proposed work is motivated to investigate novel techniques and algorithms, to alleviate spoofing consequences, without altering / re-designing GPS receiver architecture. Hence, there is a strong requirement to develop an algorithm that should address the problem of a single GPS receiver in the low observable case, which can effectively counter the GPS spoofing. Therefore, this paper introduces a novel approach of combining the epoch-by-epoch robust positioning, followed by KF, to secure the navigation track. In a particular epoch, all the pseudorange measurements (spoofed and true) available at a receiver are considered to calculate all possible positions. Later, to decrease the algorithm's complexity, the M-best position algorithm is employed, in which only M-best positions are evolved at a specific epoch by formulating a cost function based on likelihood. Once this robust positioning is performed at a specific epoch, it results in huge position estimates at an epoch, which contains both

true and spoofed positions. Interestingly, once the multiple positions are obtained at a given epoch, this navigation problem is partially modified into a well-established target tracking problem. The ambiguity of selecting one position from all the available positions, at a particular epoch, is resolved by using data association and gating technique within a Kalman filter framework.

The key contributions of the paper are as follows:

- It is proposed to accept the authentic GPS signals and spoofed GPS signals into the positioning algorithm and perform the robust positioning in a given epoch with all possible combinations of real and spoofed pseudorange measurements.
- To reduce the complexity of the proposed robust algorithm, M-best positioning algorithm is introduced based on the cost minimization problem for given measurements to form M-best likelihoods.
- The estimation of the vehicle's time-varying dynamics and removal of the unwanted position estimates is accomplished using a gating technique within the KF framework.
- The study has also explored the measurement-to-track association using nearest neighbor association and probabilistic data association.
- Moreover, the impact of proposed algorithm is also evaluated against the urban environment

The remainder of this paper is organized as follows. In the next Section II, a single GPS receiver in the spoofing environment, is formulated, along with the underlying assumption of accepting all the measurements available at a particular scan. In Section III, the iterative least squares framework for position estimation using the combinations of pseudorange measurements at a given epoch is presented, and later the M-best position algorithm is derived. Further, in Section IV, the KF framework with gating technique is described, and the data association algorithms are explored. In Section V and VI, results and discussions, and conclusions of the work are presented, respectively.

II. PROBLEM FORMULATION

This section describes GPS receiver in a clean environment, GPS receiver in spoofer only environment, and GPS receiver with an authentic and spoofed environment.

A. GPS RECEIVER IN CLEAN ENVIRONMENT

The GPS receiver uses S_i number of satellite transmitters located at $\mathbf{X}_i^t \in \mathbb{R}^3$. The satellite-based transmitted signals are $\{s_i^t(t)\}_{i=1}^I$, where I represents the number of satellites governing in the range. Here, we assumed that all the satellite transmitters are equipped with synchronized clock with no clock offset to extract the exact system time t' as given in [31]. However, this assumption is not valid in reality due to presence of clock offset in the satellites. In practice, this offset is transmitted in the navigation message, the receiver decodes the navigation message and uses the information to remove the clock offset from the measurement. The navigation signal $s_i^t(t)$ consists of satellite position, transmission timestamp, satellite health, and satellite trajectory deviation information. These satellite signals are propagated with the speed of light c and received by the GPS receiver, located at $\mathbf{x}^t \in \mathbb{R}^3$ to estimate its position. The received combined signals of all satellites in the range are

$$s^t(\mathbf{x}^t, t) = \sum_{i=1}^{I} A_i s_i^t \left(t - \frac{\mid \mathbf{X}_i^t - \mathbf{x}^t \mid}{c} \right) + w^t(\mathbf{x}^t, t). \quad (1)$$

A_i is the signal's attenuation due to the propagation of the signal from the satellite location to the target receiver. $w^t(\mathbf{x}^t, t)$ is the background noise. Due to the properties of the navigation signal $s_i(t)$, the receiver separates individual terms and extract the satellite ID, relative spreading code phase using replica of the used spreading code. Highly stable clocks like cesium oscillators are costly to employ in civilian GPS receivers. The GPS receivers cannot have two-way clock synchronization, yields in clock offset δ. The exact time at receiver is equal to summation of satellite system time and offset. Therefore, the exact time is $t = t' + \delta$. The modified received combined signals is

$$s^t(\mathbf{x}^t, t') = \sum_{i=1}^{I} A_i s_i^t \left(t - \frac{\mid \mathbf{X}_i^t - \mathbf{x}^t \mid}{c} - \delta \right) + w^t(\mathbf{x}^t, t'). \quad (2)$$

The true pseudorange measurements, corresponding to received authentic satellite signals, are given by

$$\mathbf{z}_i^t = \sqrt{(x^t - X_i^t)^2 + (y^t - Y_i^t)^2 + (z^t - Z_i^t)^2} + c\delta + n_i^t. \quad (3)$$

The received pseudorange measurement set is denoted by $\{\mathbf{z}_i^t\}_{i=1}^I$. Here $\mathbf{x}^t = [x^t, y^t, z^t]'$, $\mathbf{X}_i^t = [X_i^t, Y_i^t, Z_i^t]'$, and n_i^t is the measurement noise with zero mean Gaussian probability density function with variance $(\sigma^t)^2$. Since the pseudorange measurement consists of four unknowns, at-least four authentic satellite measurements are required to estimate three dimensional GPS receiver's location.

B. GPS RECEIVER IN SPOOFER ONLY ENVIRONMENT

The simulation of fake constillation and exact satellite time is hard. But, one can acheive this by using a meaconing technique as given in [32]. Spoofer is a device that transmits mimic GPS signals $\{s^f(t)\}_{j=1}^J$ onto the target receiver with higher power than the authentic satellite signals, to achieve easy locking into the receiver and thereby forcing the GPS receiver to wrong positioning. Let us assume that a stealthy spoofer simulates J mimic satellite signals and project them towards the target, and one cannot mitigate it using clock bias based detection technique as given in [33]. The composite signal representation of all the signals due to the presence of spoofer (fake signals) in the range is

$$s^f(\mathbf{x}^f, t') = \sum_{j=1}^{J} A_j s_j^f \left(t - \frac{\mid \mathbf{X}_j^f - \mathbf{x}^f \mid}{c} - \delta \right) + w^f(\mathbf{x}^f, t'). \quad (4)$$

Here A_j is the attenuation of the signal due to propagation from spoofer to the target and $w^f(\mathbf{x}^f, t')$ is the background noise. Here $\left\{\mathbf{X}_j^f\right\}_{j=1}^{M}$ are the set of fake satellite positions. This fake satellite position set is different from the true satellite position set due to the simulated signals, or they have captured signals at some other place or time. $\mathbf{X}^f$ is the fake location projected by the spoofer. The spoofed pseudorange measurement is given by

$$\mathbf{z}_j^f = \sqrt{(x^f - X_j^f)^2 + (y^f - Y_j^f)^2 + (z^f - Z_j^f)^2} + c\delta + n_j^f. \tag{5}$$

The received fake pseudorange measurement set is $\left\{\mathbf{z}_j^f\right\}_{i=1}^{M}$. Here $\mathbf{x}^f = \left[x^f, y^f, z^f\right]'$ and $\mathbf{X}_i^f = \left[X_i^f, Y_i^f, Z_i^f\right]'$. Due to locking of fake signals into the target receiver, the position estimation with these processed fake measurements results in spoofed locations. Even though the target is physically present at $\mathbf{x}^t$, the position estimate on account of fake pseudoranges results in $\mathbf{x}^f$ as shown in Fig. 1. The noise statistics of the spoofed pseudoranges are considered the same as true measurements, n_j^f follows white Gaussian distribution with mean zero and variance $(\sigma^f)^2$; assuming that the spoofer is ideal, and the spoofing attack cannot be detected by the signal processing techniques, like power thresholding, satellite observations, power across the individual signals, and clock bias analysis. The attenuation A_i, bias δ and noise n are same in (1) and (4) owing to ideal spoofer assumption.

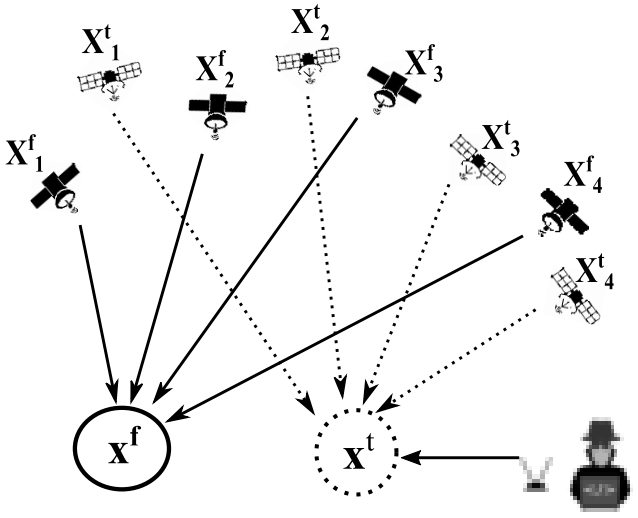

FIGURE 1. Geometry of the spoofing scenario (dotted lines represent the authentic satellite signals, dotted circle represent the true location of the target, dark lines represent the fake satellite signals, dark circle represent the fake location of the target, and the hacker).

C. GPS RECEIVER IN AUTHENTIC AND SPOOFING ENVIRONMENT

Based on the correlation of signals, the receiver receives all the available signals, and few measurements are considered for the position estimation. Here it is assumed that, the GPS receiver is receiving all the authentic and spoofed signals. The received signals in the range are expressed as a composed signal of true and spoofed signals as

$$s(t') = \sum_{k=1}^{K} s_k(t). \tag{6}$$

Here, (6) is composite form of (2) and (4). However, to avoid the ambiguity, we represented (6) in the simplified form. Here $s_k(t) \in \left\{\left\{s_i^t(t)\right\}_{i=1}^{I}, \left\{s_j^f(t)\right\}_{j=1}^{J}\right\}$. The total number of independent signals available in the composite signal is $K = I + J$. The extraction of navigation signal components from the composite signal can be obtained by spread spectrum techniques [34], [35]. For the above (6), the equivalent measurement equation is given by

$$\mathbf{z}_k = h_k(\mathbf{x}) + n_k; \quad k = 1, \ldots, K. \tag{7}$$

where

$$\mathbf{z}_k \in \left\{\left\{\mathbf{z}_i^t\right\}_{i=1}^{I}, \left\{\mathbf{z}_j^f\right\}_{j=1}^{J}\right\},$$
$$\mathbf{X}_k \in \left\{\left\{\mathbf{X}_i^t\right\}_{i=1}^{I}, \left\{\mathbf{X}_j^f\right\}_{j=1}^{J}\right\}, \text{ and}$$
$$\mathbf{x} \in \left\{\mathbf{x}^t, \mathbf{x}^f\right\}.$$

The function h has a real and non linear relation between $\mathbf{x}$ and $\mathbf{X}$. The non-linear geometry matrix is $h(\mathbf{x}) = [h_1(\mathbf{x}), \ldots h_K(\mathbf{x})]'$. Here $\mathbf{x}$ can be real position or fake position. The measurement noise vector is $n = [n_1, n_2, \ldots n_K]'$.

From K measurements, only four measurements are involved in the correlation to compute the 3D positioning. However, for 2D positioning, three measurements are adequate. Out of K measurements, I measurements are from authentic, and J measurements from the spoofer. For a given measurement, suppose the fake pseudorange probability is p, and true pseudorange probability is q. Accordingly, sum of probabilities $p + q = 1$. If L measurements are selected randomly out of available K measurements, the probability of correct solution by selecting authentic measurements from the set of received measurements is

$$\text{Probability} = \frac{{}^{I}C_L}{{}^{K}C_L}. \tag{8}$$

For example, the number of authentic measurements $I = 6$, the number of spoofed measurements in the range $J = 4$, the probability of a correct solution by selecting $L = 4$ measurements is 0.0714, which is very low. Therefore, there is a strong need to develop robust algorithms to compute all possible combinations or at least M-best combinations of measurements, and to eliminate unwanted positions to increase detection probability.

III. ROBUST POSITIONING

This section deals with the problem of position spoofing of a true target by imposing fake measurements, as shown

in Fig. 1. In this section, the robust positioning algorithm is described, and the M-best position estimates algorithm is proposed to reduce the complexity at a particular epoch.

A. ILS FRAMEWORK FOR ROBUST POSITIONING

Least squares is the most popular technique in determined and overdetermined systems. Usually, in GPS positioning, the number of pseudorange equations are more than the unknowns to be estimated or some times equal. LS usually solves the whole set to offer a solution that minimizes the sum of squared errors. In LS estimation, linear LS and non-linear LS solutions exist. The closed-form of the solution is linear LS, and iterative refinement of the solution is non-linear LS. Considering the user position $\mathbf{x} = [x, y, z]'$, the position $\mathbf{x} \in \{\mathbf{x}^t, \mathbf{x}^f\}$ depends on the tuple of measurements considered from all possible pseudoranges, arrived due to true and spoofed measurements. The generalized pseudorange measurement equation combining (3) and (5) is given by

$$\begin{aligned}\mathbf{z}_k &= h_k(\gamma) + n_k, \\ &= \sqrt{(x - X_k)^2 + (y - Y_k)^2 + (z - Z_k)^2} + ct + n_k. \quad (9)\end{aligned}$$

To solve the above nonlinear equation using LS technique, $\mathbf{z}_k$ has to be linearized using Taylor series expansion around the approximate user position $[\hat{x}, \hat{y}, \hat{z}]'$. Defining $\hat{\mathbf{z}}_k$ as $\mathbf{z}_k$ at $[\hat{x}, \hat{y}, \hat{z}]'$ can be written as

$$\begin{aligned}\mathbf{z}_k = \hat{\mathbf{z}}_k + \frac{\partial \mathbf{z}_k}{\partial x}\,|_{(\hat{x},\hat{y},\hat{z})}\,(x - \hat{x}) + \frac{\partial \mathbf{z}_k}{\partial y}\,|_{(\hat{x},\hat{y},\hat{z})}\,(y - \hat{y}) \\ + \frac{\partial \mathbf{z}_k}{\partial z}\,|_{(\hat{x},\hat{y},\hat{z})}\,(z - \hat{z}) + H.O.T + ct + n_k. \quad (10)\end{aligned}$$

Here, H.O.T is the higher-order terms in the Taylors series expansion. The higher-order terms are ignored in further calculations, and the resultant is the linear approximation to (9). Let $\Delta x = x - \hat{x}$, $\Delta y = y - \hat{y}$, $\Delta z = z - \hat{z}$. The partial derivatives are given by

$$\begin{aligned}\frac{\partial \mathbf{z}_k}{\partial x} &= \frac{X_k - x}{\hat{\mathbf{z}}_k}, \\ \frac{\partial \mathbf{z}_k}{\partial y} &= \frac{Y_k - y}{\hat{\mathbf{z}}_k}, \quad \text{and} \quad (11) \\ \frac{\partial \mathbf{z}_k}{\partial z} &= \frac{Z_k - z}{\hat{\mathbf{z}}_k}.\end{aligned}$$

The resultant equation after substituting the partial derivatives is

$$\mathbf{z}_k - \hat{\mathbf{z}}_k = \frac{X_k - x}{\hat{\mathbf{z}}_k}\Delta x + \frac{Y_k - y}{\hat{\mathbf{z}}_k}\Delta y + \frac{Z_k - z}{\hat{\mathbf{z}}_k}\Delta z + ct + n_k. \quad (12)$$

In the above, replace $\Delta \mathbf{z}_k = \mathbf{z}_k - \hat{\mathbf{z}}_k, h_{x_k} = \frac{X_k - x}{\hat{\mathbf{z}}_k}, h_{y_k} = \frac{Y_k - y}{\hat{\mathbf{z}}_k}$, and $h_{z_k} = \frac{Z_k - z}{\hat{\mathbf{z}}_k}$. Where h_{x_k}, h_{y_k}, and h_{z_k}, are direction cosines of unit vector pointing from approximate GPS position to the k^{th} satellite. The unit vector is given by $h_k = \begin{bmatrix} h_{x_k} & h_{y_k} & h_{z_k} & 1 \end{bmatrix}$. H is a geometry matrix, given by $H = [h_1, \ldots, h_L]'$ The linearized measurement model is given by

$$\Delta \mathbf{z} = H\gamma + n, \quad (13)$$

where $\Delta \mathbf{z}$ is a measurement vector to represent the difference between actual pseudorange measurement and computed pseudorange measurement, i.e., $\Delta \mathbf{z} = [\Delta \mathbf{z}_1, \ldots, \Delta \mathbf{z}_L]'$. $\gamma = [\Delta \mathbf{x}, \delta]'$ is a vector of unknown parameters to be estimated, and n is a pseudorange measurement error vector, given by $n = [n_1, \ldots, n_L]'$. For (13), linear model exists and the noise vector n has Gaussian distribution with zero mean and covariance C. The best linear unbiased estimator (BLUE) of position is

$$\hat{\gamma} = (H'C^{-1}H)^{-1}H'C^{-1}\Delta \mathbf{z}. \quad (14)$$

The covariance of the estimator is given by

$$R = H'C^{-1}H. \quad (15)$$

This LS algorithm can run iteratively by using the old position estimates to estimate the new positions. In the above equation, once the unknowns are computed, these unknowns can be used to obtain the new estimates $\hat{x}$, $\hat{y}$, and $\hat{z}$. The iterative least squares (ILS) has termination criteria based on the maximum number of iterations or based on the maximum amount of correction.

At a given epoch with K pseudoranges (true and spoofed), this ILS runs ${}^{K}C_{L}$ times to produce ${}^{K}C_{L}$ position estimates, in which ${}^{I}C_{L}$ are true position estimates and rest are spoofed position estimates as shown in the Fig. 2. Here in the given Fig. 2, The bottlenecks of this robust algorithm are complexity and decision making. The complexity of the robust algorithm increases exponentially with every single injection of spoofed pseudorange. we can clearly see that the true position estimates are forming a cluster and similarly fake position estimates creating another cluster. Consider an example with $I = 5$ and $J = 5$ to understand the problem clearly. In this case, ${}^{I}C_{4}$ true position estimates are available

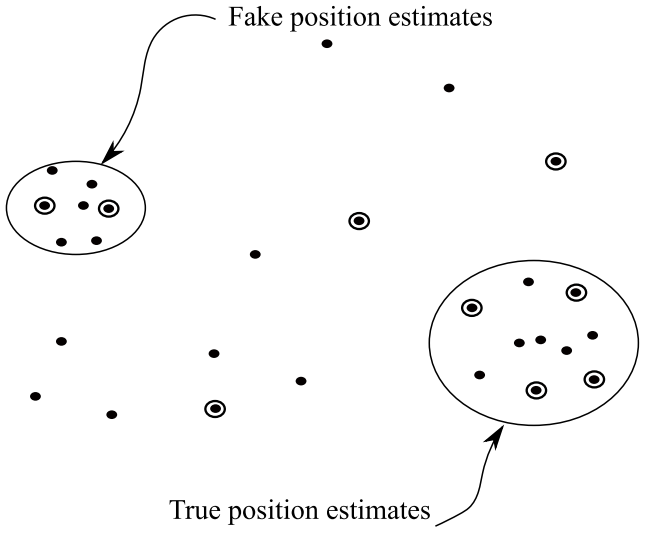

FIGURE 2. Robust positioning by considering all possible solutions and M-best solutions at a given epoch in GPS spoofing scenario (Black dots are the position estimates due to robust positioning and circles are the position estimates due to M-best estimation algorithm).

in true cluster and ${}^{J}C_4$ position estimates are present in fake cluster. The remaining number of ${}^{K}C_4-({}^{I}C_4+{}^{J}C_4)$ estimates are biased estimates neither fall in true cluster nor fake cluster. So, the algorithm should be intelligent enough to compute M-best pseudorange sets from the given scan of measurements rather than finding all the possible combinations. After that, for the best sets, the ILS algorithm computes position estimates as presented in Section III-B. It is very hard to decide which cluster of positions belong to true positions. Hence, there is a need to discard unwanted position estimates from the given estimates.

B. M-BEST POSITIONING ALGORITHM

In a given scan of measurements (true and spoofed), the spoofer simulated measurements are totally different from the authentic satellite measurements by satellite ID, or few spoofer simulated signals match with the authentic satellite signals, thus the measurement set is given as

$$\begin{Bmatrix} \mathbf{z}_1^t, & \cdots, & \mathbf{z}_i^t, & \cdots, & \mathbf{z}_j^t, & \cdots, & \mathbf{z}_J^t, & 0, & 0, & 0 \\ 0, & 0, & \mathbf{z}_i^f, & \cdots, & \mathbf{z}_j^f, & 0, & 0, & \mathbf{z}_1^f, & \cdots, & \mathbf{z}_J^f \end{Bmatrix}$$

Here, the measurement index i to j have the same satellite ID. Hence there exist total of S active satellites, where $S \leq K$ and $s = 1, 2, \cdots, S$. We wish to associate the observations from S lists of n_s measurements. For a single spoofed signal case, $n_s = 3$, since $\{\mathbf{z}_{i_s}^t, \mathbf{z}_{i_s}^f, 0\}$, here zero is the dummy variable. The index $i_s = 1, 2, \cdots, n_s$. The measurement corresponding to every index i_s is with detection probability either one or zero.

$$PD_{\zeta(i_s)} = \begin{cases} 0, & \text{if} \quad \mathbf{z}_{i_s} = 0, \\ 1, & \text{otherwise.} \end{cases} \tag{16}$$

Here, the source may be an authentic satellite, then the true measurements are assumed to be a function of the true state and the additive measurement noise is as given in (3). Whereas, in case the source is a spoofer, the spoofed measurements are assumed to be a function of the spoofed state and the additive measurement noise is as given in (5). The problem is formulated as a multi-sensor state estimation problem with association and estimation. Association is the process of linking the measurements, and the linked measurements are filtered with estimation. Thus, the measurements have been selected in such a way that one measurement is selected from each index. The measurement index is appended to the dummy variable of zero. This problem is commonly seen in assignment problem formulations in multi-sensor multi-target scenarios [36]. Here estimation refers to position estimate by using pseudorange algorithms. The target state uniquely determines as a true position or spoofed position. For convenience, the target state is given by $\mathbf{x} \in \{\mathbf{x}^t, \mathbf{x}^s\}$. To associate the list of measurements obtained for sources $\zeta(s) \in [1, 2, \ldots S]$, where $\zeta(i_s)$ is the source of measurement either generated by satellite or spoofer. Let the selection of measurement from i_s index be $\mathbf{z}_{i_s}$. Where $\mathbf{z}_{i_s} \in \{\mathbf{z}_{i_s}^t, \mathbf{z}_{i_s}^f, \mathbf{z}_o\}$. The measurement $\mathbf{z}_{i_s}$ either originated from satellite or spoofer or missed detection (zero measurement), in which case, weather true or fake it is taken as $H(\mathbf{x}, \mathbf{X}_{i_s})$ plus some additive white Gaussian noise. Besides, each $\zeta(i_s)$ has a known detection probability $PD_{\zeta(i_s)}$ and it depends on the characteristics of the signal as given in (16).

The likelihood of S-tuple of measurements $\mathbf{z} = \{\mathbf{z}_1, \ldots, \mathbf{z}_L\}$ originating from target $\mathbf{x}$ is

$$\Lambda(\mathbf{z}_{i_1}, \ldots, \mathbf{z}_{i_S} \mid \mathbf{x}) = \prod_{s=1}^{S} [1 - PD_{\zeta(i_s)}]^{1-u(i_s)} \times [PD_{\zeta(i_s)} p\left(\mathbf{z}_{i_s} \mid \mathbf{x}\right)]^{u(i_s)}. \tag{17}$$

The likelihood of set of measurements are spurious with $\psi_{\zeta(i_s)}$ as a field of view for sensor $\zeta(i_s)$ is given by

$$\Lambda(\mathbf{z}_{i_1}, \ldots, \mathbf{z}_{i_S} \mid \mathbf{x} = \phi) = \prod_{s=1}^{S} \left[\frac{1}{\psi_{\zeta(i_s)}}\right]^{u(i_s)}. \tag{18}$$

$u(i_s)$ is a indicator function, given by

$$u(i_s) = \begin{cases} 0, & \text{if } \mathbf{z}_{i_s} = 0, \\ 1, & \text{otherwise.} \end{cases} \tag{19}$$

The cost of associating the set of measurements to target $\mathbf{x}$ is defined with negative log likelihood ratio

$$C_{i_1,\ldots,i_S} = -\ln \frac{\Lambda(\mathbf{z}_{i_1}, \ldots, \mathbf{z}_{i_S} \mid \mathbf{x})}{\Lambda(\mathbf{z}_{i_1}, \ldots, \mathbf{z}_{i_S} \mid \mathbf{x} = \phi)}. \tag{20}$$

However, $\mathbf{x}$ is unknown and replaced by maximum likelihood estimate $\hat{\mathbf{x}}^{ML}$. The likelihood can be written as

$$\begin{aligned} \Lambda(\mathbf{Z} \mid \mathbf{x}) &= \Lambda(\mathbf{z}_{i_1}, \ldots, \mathbf{z}_{i_S} \mid \mathbf{x}), \\ &= \left(\frac{1}{\sqrt{2\pi\sigma}}\right)^{S} \exp\left(\frac{-1}{2\sigma^2} \sum_{s=1}^{S} [\mathbf{Z} - h][\mathbf{Z} - h]'\right), \end{aligned} \tag{21}$$

where $\sigma = \sigma^t = \sigma^f$ from ideal spoofer assumption. Here $\mathbf{Z} = [\mathbf{z}_{i_1}, \ldots, \mathbf{z}_{i_S}]'$ and $h = [h_{i_1}, \ldots, h_{i_S}]$. Similarly the log likelihood is written as

$$\ln \Lambda(\mathbf{Z} \mid \mathbf{x}) = \left[\frac{-1}{2\sigma^2} \sum_{s=1}^{S} [\mathbf{Z} - h][\mathbf{Z} - h]'\right]. \tag{22}$$

Therefore maximizing the log likelihood is given by

$$\begin{aligned} \hat{\mathbf{x}}^{ML} &= \arg\max \left[\frac{-1}{2\sigma^2} \sum_{s=1}^{S} [\mathbf{Z} - h][\mathbf{Z} - h]'\right], \\ &= \arg\min \left[\sum_{s=1}^{S} [\mathbf{Z} - h][\mathbf{Z} - h]'\right]. \end{aligned} \tag{23}$$

Therefore, the cost of associating the measurements to target $\mathbf{x}$ is

$$C_{i_1,\ldots,i_S} = \sum_{s=1}^{S} [u(i_s) - 1] \ln[1 - PD_{\zeta(i_s)}] - u(i_s) \ln\left(\frac{PD_{\zeta(i_s)} \psi_{\zeta(i_s)}}{\sqrt{2\pi\, \Sigma_{\zeta(i_s)}}}\right)$$

$$+u(i_s)\times\frac{1}{2}\left[\mathbf{z}_{i_s}-h_{i_s}\left(\hat{\mathbf{x}}^{ML}\right)\right]'\Sigma^{-1}_{\zeta(i_s)}\times\left[\mathbf{z}_{i_s}-h_{i_s}\left(\hat{\mathbf{x}}^{ML}\right)\right]. \quad (24)$$

The main goal of this formulation is to get most likely set of S-tuples such that either the measurement assigned to target or declared as false by taking at most one measurement from each list. This can be reformulated as a well known optimization problem of S-D assignment in multi-sensor multi-target as

$$\min_{\xi_{i_1 i_2\cdots i_S}}\sum_{i_1=1}^{n_s}\sum_{i_2=1}^{n_s}\cdots\sum_{i_S=1}^{n_s}C_{i_1 i_2\cdots i_S}\xi_{i_1 i_2\cdots i_S} \quad (25)$$

subjected to

$$\sum_{i_2=1}^{n_s}\cdots\sum_{i_S=1}^{n_s}\xi_{i_1 i_2\cdots i_S}=1;\quad i_1=1,\cdots n_s$$
$$\sum_{i_1=1}^{n_s}\cdots\sum_{i_S=1}^{n_s}\xi_{i_1 i_2\cdots i_S}=1;\quad i_2=1,\cdots n_s$$
$$\vdots\qquad\qquad\vdots$$
$$\sum_{i_1=1}^{n_s}\cdots\sum_{i_{S-1}=1}^{n_s}\xi_{i_1 i_2\cdots i_S}=1;\quad i_S=1,\cdots n_s$$

where, $\xi_{i_1 i_2\cdots i_S}$ are binary association variables such that $\xi_{i_1 i_2\cdots i_S}=1$ if the S-tuple is associated with true target or spoof target. Otherwise, it is set to zero. The above assignment problem (24) solved using the murthy assignment algorithm [37], [38], and M-best costs are selected in this algorithm which in turn results in M-best positions.

Now the position estimates $\{\hat{\mathbf{x}}_l\}_{l=1}^{M}$ evolved at a given epoch are the observations to the KF based estimator. Hence, these position estimates are being redefined, as observations to avoid the confusion in the next section, i.e., $y=\{y_l\}_{l=1}^{M}=\{\hat{\mathbf{x}}_l\}_{l=1}^{M}$. This M-best gives results of robust positioning by giving value of M equals to ${}^{K}C_{L}$.

IV. KALMAN FILTERING AND DATA ASSOCIATION

In this section, trajectory spoofing problem is presented. Initially, how the spoofer misleads the true trajectory of the target is explored and then the navigation filter solution is presented.

A. TRAJECTORY SPOOFING

The final goal of spoofer in trajectory spoofing is to mislead the true target trajectory by continuously imposing the false measurements and change the destination of the target. An abrupt positioning by the spoofing effect can be easily detected by using a normalized innovation square test (NIS) or gating technique. So the ideal spoofer must possess a strategy to mislead the target. Here, we are dealing with the spoofing technique namely position gate pull-off [39]. The stealthy trajectory spoofing involves three phases, i.e., carry-off, deceive, and hand-off. In the carry-off phase, the projected spoofed location and the true location of the target almost coincide with each other for a certain duration of the time. The spoofing starts at $t(o)$, replicates the target position for the time duration of T, as shown in Fig. 3. During this interval, the spoofer boosts the spoofed signal to capture the receiver. Once the target is captured by the spoofer, the second phase of spoofing is called as deceiving starts. Deceiving is slightly moving the spoofed location from the actual true location with lower turn rates. After a time duration of T, the spoofer generates measurements in such a fashion so as to separate the target from the planned path with any realistic trajectory models. During this phase, if the autonomous vehicles are more reliable on the inertial navigation system (INS) rather than the GPS, one can move the spoofed trajectory with very small deviations because the IMU sensors are incapable of detecting the lower turn rates for successful spoofing in such cases [40]. Once the target totally relies on the spoofed trajectory, the target can lead to a phase called hand-off, as shown in Fig. 3. The algorithms should be intelligent enough to resolve the issue during this deception phase.

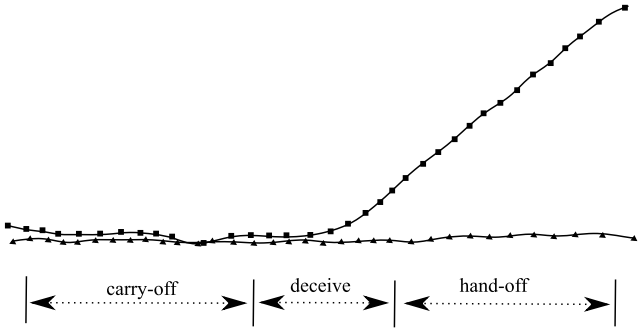

FIGURE 3. Different stages of spoofing attack to deceive the navigation track.

The mathematical model for position pull-off based trajectory generation [39] is given by

$$\mathbf{x}^f(m)=\begin{cases}\mathbf{x}^t(m); & t(m)\le t(o)+T,\\ \mathbf{x}^f(m-1)+v_o(\Delta t); & t(m)>t(o)+T,\end{cases} \quad (26)$$

where m is a discrete time index, v_0 is velocity vector. Here sampling time $\Delta t=t(m)-t(m-1)$. For a selected values of vector v_0, the spoofed target can follow any trajectory models.

Let the spoofed trajectory state be $X^f=\left[\mathbf{x}^f\ \dot{\mathbf{x}}^f\right]'$, where $\dot{\mathbf{x}}^f$ is the velocity vector. The dynamic state equation is given by

$$X^f(m)=FX^f(m-1)+\Gamma u(m-1), \quad (27)$$

where F is a state transition matrix and Γ is a noise gain matrix. The F can follow constant velocity (CV) model F_{CV} or constant turn (CT) model F_{CT} as given in [41]. The u follows Gaussian with zero mean and covariance Q.

$$F_{CV}=\begin{bmatrix}1&0&0&\Delta t&0&0\\0&1&0&0&\Delta t&0\\0&0&1&0&0&\Delta t\\0&0&0&1&0&0\\0&0&0&0&1&0\\0&0&0&0&0&1\end{bmatrix},$$

where Δt is the sampling time.

$$F_{CT} = \begin{bmatrix} 1 & 0 & \frac{\sin\omega\Delta t}{\omega} & -\frac{1-\cos\omega\Delta t}{\omega} & 0 \\ 0 & 1 & \frac{1-\cos\omega\Delta t}{\omega} & \frac{\sin\omega\Delta t}{\omega} & 0 \\ 0 & 0 & \cos\omega\Delta t & -\sin\omega\Delta t & 0 \\ 0 & 0 & \sin\omega\Delta t & \cos\omega\Delta t & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix},$$

where ω is the turn rate. The noise gain matrix is given by

$$\Gamma = \begin{bmatrix} \frac{\Delta t^2}{2} & 0 & 0 \\ 0 & \frac{\Delta t^2}{2} & 0 \\ 0 & 0 & \frac{\Delta t^2}{2} \\ \Delta t & 0 & 0 \\ 0 & \Delta t & 0 \\ 0 & 0 & \Delta t \end{bmatrix},$$

the covariance corresponding to this noise gain matrix is $Q = \Gamma'\sigma^2\Gamma$.

B. KALMAN FILTERING

For a discrete time linear dynamic system the plant equation is consider as

$$X(m+1) = F(m)X(m) + \Gamma u(m). \tag{28}$$

Here m is a discrete time instant. $X(m)$ is a state with n_X dimension, and $u(m)$ is process noise which is Gaussian with mean zero whose covariance is given as $E\left[u\,(m)\,u\,(m)'\right] = Q\,(m)$. Where, $E[\cdot]$ is an expectation. The observation is given by

$$y(m) = \begin{cases} H(m)X(m) + w(0, R(m)), & \text{true origin,} \\ \{FA_l(m)\}_{l=1}^{M-1}, & \text{spoofed.} \end{cases} \tag{29}$$

where $y(m)$ consists of positions related to true, spoofed, and bias. FA is false alarms representing the spoofed positions. Since the observations and state are in positions, the measurement transition matrix is linear. w is zero-mean white Gaussian with covariance $R(m)$ as derived in (15). The values of F (state transition matrix), H (measurement matrix), R (measurement noise covariance), and Q (process noise covariance) are assumed to be known and vary with time. The state prediction is

$$\hat{X}\,(m+1|m) = F\,(m)\,\hat{X}\,(m|m)\,. \tag{30}$$

The measurement prediction is

$$\hat{y}\,(m+1|m) = H\,(m+1)\,\hat{X}\,(m+1|m)\,. \tag{31}$$

The Covariance of the predicted state is

$$P\,(m+1|m) = F\,(m)\,P\,(m|m)\,F\,(m)' + Q\,(m)\,. \tag{32}$$

Similarly, the innovation covariance is given by

$$S\,(m+1) = H\,(m+1)\,P\,(m+1|m)\,H\,(m+1)' \tag{33}$$

$$+ R\,(m+1)\,. \tag{34}$$

The Kalman gain is given by

$$G(m+1) = P(m+1|m)H(m+1)S(m+1)^{-1}. \tag{35}$$

All the above equations are the same as in standard KF used in navigation. Nevertheless, in navigation, only one measurement is available to update the state and covariance. Either all possible positions or M-best positions are calculated; in both cases, a large number of observations are evolved, as is the case of a typical tracking scenario. Consider a scenario with four authentic measurements, four spoofed measurements, and four appended dummy variables. Evaluating the combinations (based on four authentic, four spoofed measurements, and four appended dummy variables) yields to eighty-one combinations. Out of these, only fifteen best positions are taken and plotted as seen in Fig. 4.

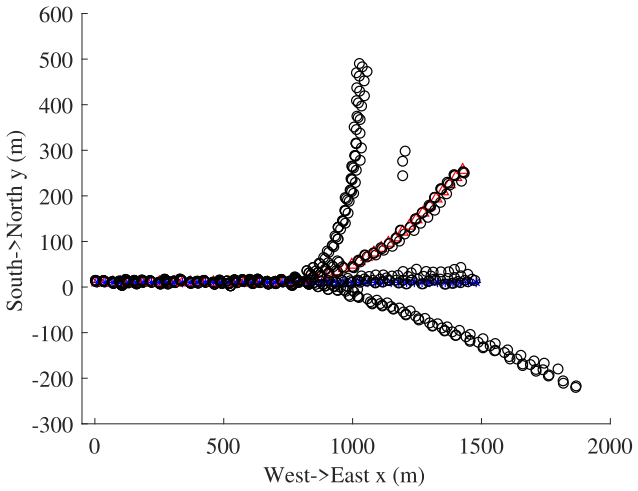

FIGURE 4. Navigation tracks in spoofing (I=4, J=4, K=4, and M-best=15).

In the initial phase of carry-off, all the M-best estimates forms a single cluster, hence there is no ambiguity for measurement-to-track association. Whereas, it is clearly evident that evolved M-best estimates during the deceiving phase are not forming a single cluster, which leads to ambiguity of measurement-to-track association. Further, once the track is associated with wrong measurements, true trajectory follows the fake estimate and carried away by the spoofer. A gating technique is performed with in the filter framework to resolve this issue of selecting few estimates from the M-best estimates. The validation region (gate) is ellipsoid given by

$$\mathcal{V}\,(m+1) = \left\{ y : v(m+1)'S\,(m+1)^{-1}\,v(m+1) \le \xi^2_{n_y} \right\}, \tag{36}$$

where ξ is the gate threshold determined by the chosen gate probability P_G. The ξ follows a chi-square distribution with a n_y degree of freedom and given tail probability. For 2D and 3D case n_y is equal to two and three respectively. The valid measurements falling within the gate are $\{y_l\}_{l=1}^{L^*}$. In a given M observations, only L^* observations falling within the gate, at the given discrete time instant. The innovation

corresponding to the l^{th} validated measurement is represented as

$$v(m+1) = y_l - \hat{y}(m+1|m); \quad l = 1, \ldots, L^*(m+1). \quad (37)$$

The updated state is given by

$$\hat{X}(m+1|m+1) = \hat{X}(m+1|m) + G(m+1)\, v(m+1). \quad (38)$$

Similarly, the updated covariance corresponding to the state is given by

$$P(m+1|m+1) = P(m+1|m) - G(m+1)S(m+1)G(m+1)^{-1}. \quad (39)$$

C. POSITION TO TRACK ASSOCIATION

The data associations employed in this KF is the nearest neighbor (NN) and probabilistic data association (PDA) [41]. In NN, the nearest observation to the predicted track is considered, and the innovation is carried out using this observation. Whereas, in PDA probability of l^{th} validated measurements considered, to find the correct one be

$$\beta_l(m+1) = \begin{cases} \dfrac{e_l}{1 - P_D P_G + \sum_{l=1}^{L^*(m+1)} e_l}, & l = 1, \ldots, L^*(m+1), \\ \dfrac{1 - P_D P_G}{1 - P_D P_G + \sum_{l=1}^{L^*(m+1)} e_l}, & l = 0. \end{cases} \quad (40)$$

$\beta_0(m+1)$ is association probability, which shows that none of the measurement is correct. The likelihood ratio e_l is given by

$$e_l \triangleq \exp\left(-\frac{1}{2} v_l(m+1)' S(m+1)^{-1} v_l(m+1)\right). \quad (41)$$

whereas P_D is the probability of detection and P_G is the gating probability. The updated state is given by

$$\hat{X}(m+1|m+1) = \hat{X}(m+1|m) + G(m+1)\, v(m+1). \quad (42)$$

with the combined innovation as

$$v(m+1) \triangleq \sum_{i=1}^{L^*(m+1)} \beta_i(m+1)\, v_i(m+1). \quad (43)$$

The Updated covariance is given as

$$P(m+1|m+1) = P(m+1|m) - [1 - \beta_0(m+1)] \times G(m+1)\, S(m+1)\, G(m+1)'. \quad (44)$$

V. RESULTS AND DISCUSSIONS

This section presents scenario generation, design parameters, and robustness of the proposed algorithm. To illustrate the robustness of the proposed algorithm, different scenarios like open space (LOS measurements with $I = 4$ to $I = 6$) and a multi-path environment (Non-LOS measurements with $I = 4$) are examined.

A. SCENARIO GENERATION

The satellite trajectories are modeled using WGS-84, and follows an assumption of circular orbits as

$$X(t) = R\left[\cos\theta(t)\cos\Omega(t) - \sin\theta(t)\sin\Omega(t)\cos 55^o\right]$$
$$Y(t) = R\left[\cos\theta(t)\sin\Omega(t) + \sin\theta(t)\cos\Omega(t)\cos 55^o\right]$$
$$Z(t) = R\sin\theta(t)\sin 55^o.$$

Here $\mathbf{X} = [X, Y, Z]'$ is the satellite positional information, R is the radius ($R = 26,560$ Km) of circular orbit, Ω and θ are right ascension and angular phase in the circular orbit respectively.

$$\Omega(t) = \Omega(0) - (t - t(0))\left(\frac{360}{86164}\right)^o$$
$$\theta(t) = \theta(0) + (t - t(0))\left(\frac{360}{43082}\right)^o$$

The true satellite positions are collected at $t(0)$ instant, processed and re-transmitted at the same instant. Hence, the anti-spoofing algorithm like constellation check cannot detect the spoofing effect [11]. The initial positions of the satellite are given in Table 1

TABLE 1. The satellite initial positions (angles $\theta(0)$ and $\Omega(0)$).

N	1	2	3	4	5	6
$\theta(0)$	325.7	25.7	85.7	145.7	205.7	265.7
$\Omega(0)$	72.1	343.9	214.9	211.9	93.9	27.9

We consider a position pull-off spoofing technique test bench trajectory [39] to evaluate the proposed algorithm. The initial state vector of the true target is $\mathbf{x}^t(0) = [10, 10, 10]'$ and its velocity vector $\dot{\mathbf{x}}^t(0) = [30, 0, 0]'$. The target moves towards the east (x) throughout the simulation with 30 m/s for 80 s with a CV model. The target trajectory consists of ideal trajectory and turbulence; the turbulence is modeled as process noise, follows Gaussian with zero mean and the standard deviation vector is given by $[0.05, 0.05, 0, 0.02, 0.02, 0]'$. The first three elements of the standard deviation vector represent the position, and the other three elements correspond to velocity. The process noise exists along x and y directions, and absent in z direction due to the ground moving target assumption.

The spoofing process starts at $t = 21$ s and follows till the end. Since the target is not being influenced until $t = 21$ s, the standard navigation solution exists during this non-spoofing phase. The spoofed trajectory follows both CV and CT models, as presented in critical examples [22]. From 21 s, the carry-off phase starts with CV model and carried out for a further duration of 20 s. After that, the deceiving phase starts and lasts for 20 s, by taking left CT with $\omega = 1^o$/s. Thereafter, the hand-off phase is carried out with the CV model for another 20 s duration as shown in Fig. 5.

B. DESIGN PARAMETERS

Since the ideal spoofer is considered in this paper, spoofer can process the spoofed pseudorange measurements with the

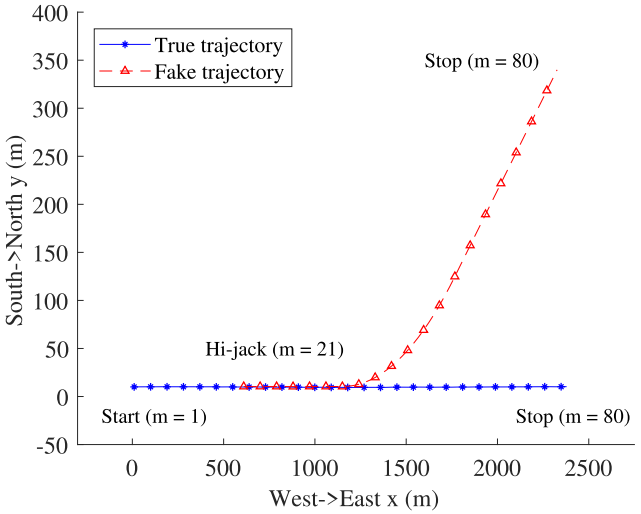

FIGURE 5. True and fake trajectory generation (True - target planned trajectory, fake - Spoofer imposing trajectory on target).

same noise as of true pseudoranges. Both the pseudorange measurements are corrupted by white Gaussian noise with standard deviation, i.e., $\sigma_i^t = \sigma_j^f = 1$ m. The sampling time of KF is $\Delta t = 1$ s. Two-point initialization method [41] is used to initialize the filter. If the spoofing is carried out from the initial timestamp, the same two-point initialization method can be applied with the values of means of a cluster. The means of the cluster of positions formed at $t(0)$ and $t(1)$ epoch are $\mathbf{x}_\mu^t(0)$ and $\mathbf{x}_\mu^t(1)$ respectively. The state vector is

$$X(1) = \left[\hat{x},\ \hat{y},\ \hat{z},\ \dot{\hat{x}},\ \dot{\hat{y}},\ \dot{\hat{z}}\right]' = \left[\mathbf{x}_\mu^t(1),\ \frac{\mathbf{x}_\mu^t(1) - \mathbf{x}_\mu^t(0)}{t(1) - t(0)}\right]'. \quad (45)$$

The state transition matrix in the filter design is F_{CV} and the noise gain is Γ. The measurement transition matrix is given by $H = [I_3\ 0_3]$, where I_3 represents the identity matrix and 0_3 is the zero matrix with dimension three. Moreover, the process noise covariance of the filter is initialized using the CRLB as given in [42]. To resolve the ambiguity of observation to track, NN and PDA techniques are deployed.

C. ROBUSTNESS OF ALGORITHM

The robustness of the algorithm is verified by varying the number of authentic signals and spoofed signals available at the receiver. Here, the robustness is evaluated for open space environment and urban environment. Open space environment implies that there are no multi-path measurements in the received set. Whereas, the urban environment introduces multi-path measurements in the authentic set. The position root mean square error (PRMSE) and track swap (TS) are the two quantifying measures considered in this paper. The TS is defined as the deceiving of navigation track from the true trajectory.

1) OPEN SPACE ENVIRONMENT

Assuming that the GPS receiver is located in low visibility scenario with $I = 4$ authentic satellite signals. Here all the signals are LOS with the receiver without any multi-path. In this case, a determined solution (number of unknowns to be estimated, equal to the number of available pseudoranges) exists for navigation. In the presence of spoofing, in addition to four true satellite signals, the spoofed signals are introduced with a variable number of $J = 1, \ldots, 6$. Here, during the initial phase of trajectory $m \in [1, 20]$, the navigation filter follows a true trajectory without any spoofing. Due to the lack of initial velocity of the filter, two-point initialization is used, a decrease is seen in PRMSE of navigation filter after initialization, till $m = 20$ s. Thereafter, the carry-off phase is implemented for $m \in [21, 40]$, in which both true and spoofed trajectories follow the same path. Even though huge measurement-to-measurement associations occur in this interval, insignificant deflection in PRMSE is observed, as depicted in Fig. 6 (since trajectories are aligned to each other). Whereas, in the interval of deceiving $m \in [41, 60]$, numerous observations are generated. M-best algorithm produces only M limited observations. From these M observations, selecting a single measurement for measurement-to-track association is a difficult process. Hence, this problem is addressed by deploying NN data association technique. Since NN is employed, the filter selects the nearest observation and updates the filter. In this process, as the number of spoofed injections increases, PRMSE and TS values increases as shown in Figs. 6, 7, and 8. This is because, as number of spoofed injections increases, the measurement-to-track association ambiguity increases. As NN is a hard decision, once the track is decepted with the false measurement, it is hard to get back to the true trajectory path, and estimated path would continue to be with false measurements. Therefore, the increase in ambiguity of measurement-to-track association with number of spoof injections can be intuitively related

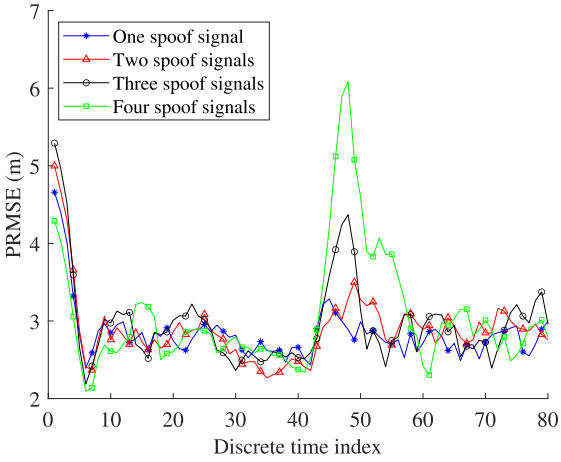

FIGURE 6. PRMSE for fixed four authentic satellite signals and variable number of spoofed signal injections with nearest neighbour association (MC = 100).

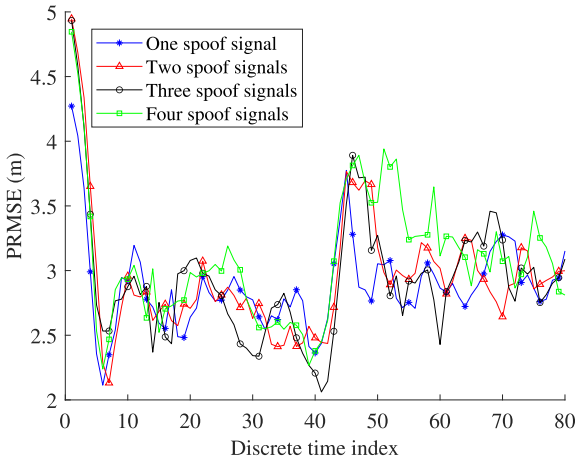

FIGURE 7. PRMSE for fixed five authentic signals and variable number of spoofed signal injections with nearest neighbor association (MC = 100).

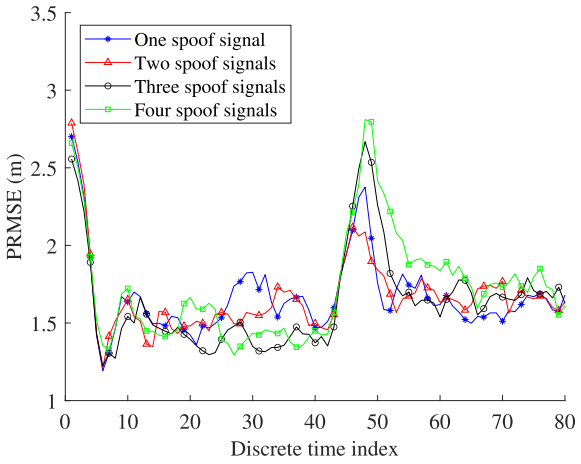

FIGURE 8. PRMSE for fixed six authentic signals and variable number of spoofed signal injections with nearest neighbor association (MC=100).

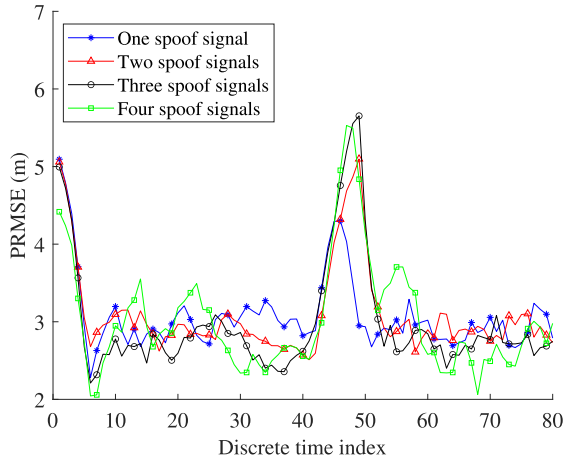

FIGURE 9. PRMSE for fixed four authentic satellite signals and variable number of spoofed signal injections with probabilistic data association (MC = 100).

with the increase in PRMSE value during the deception phase and is clearly shown in Figs. 6, 7, and 8. In this deceiving phase, the navigation filter chooses either the true trajectory or the spoofed trajectory depending on the data association. If the target tends to follow the spoofed trajectory, it follows until the end, which is considered as TS. During the hand-off phase $m \in [61, 80]$, the clusters of observations are totally separable and the filter follows any one of the track, and hence PRMSE settles down as illustrated in Figs. 6, 7, and 8. The selection of M value in the algorithm is very crucial. So always the value of M set to number of available satellite signals. However one can vary the value of M and see the overall performance of the algorithm.

In another scenario, the GPS receiver receives $I = 5, 6$ authentic satellite signals. The available true ranges are greater than the number of parameters to be estimated, and the solution becomes over-determined. The spoofed signal injections vary as $J = 1, \cdots, 6$. During the carry-off phase, we can observe improved PRMSE compared to the $I = 4$ case. This is due to the total number of ranges being involved in the position estimation and also because of the dummy variable assignment in the algorithm, the M-best solution gives positions related to all authentic satellite measurements. Due to the increase of measurements, there is a huge measurement-to-measurement association in this phase compared to the $I = 4$ scenario, and is computationally expensive. In the Fig. 7 and 8, an improved PRMSE is observed in the deceiving phase, compared to that of Fig. 6. The improved PRMSE is due to more number of authentic satellite signals involved in the ILS solution, compared to the $I = 4$ case. During the deception phase, the TS is decreased in comparison to four authentic satellite cases; this is because of either an increase in the position integrity or lesser ambiguity of selecting an observation within the gate. The TS is reported in Table 2; an increase in true measurements improves the navigation filter to choose the true trajectory rather than fake trajectory. The TS rate increases as the number of injections increase, as shown in Table 2. Similar to the previous case, the clusters are well separated in the interval of hold off, and the PRMSE settles down as shown in Fig. 8. The simulations are carried out for five authentic measurements and its corresponding spoofed measurement injection, and the TS are depicted in Table 2.

The drawback of the NN is its hard decision towards measurement-to-track association, by considering the nearest observation. So, the probabilistic data association is used for the above-stated problem. Interestingly, owing to PDA, the TS is decreasing compared to NN technique. If wrong measurement-to-track association is taken place in the initial stage of deception, there is a highly likelihood that it will get corrected, since PDA evaluate all weighted measurements within the gate to form the innovation. The number of TS by varying the authentic and spoofed signals is presented in Table 2. But, during the interval of carry-off phase, a little raise is seen in PRMSE, by using PDA technique. Since

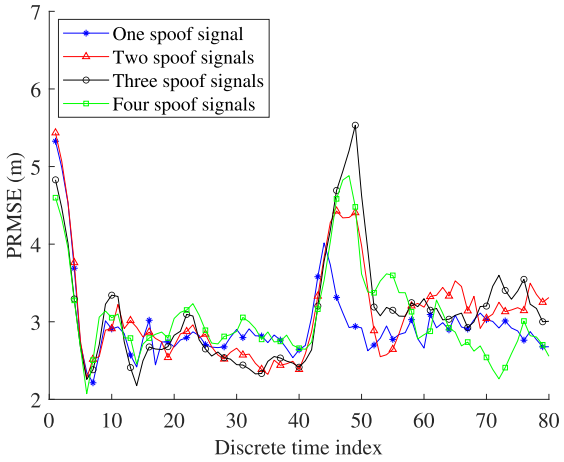

FIGURE 10. PRMSE for fixed five authentic signals and variable number of spoofed signal injections with probabilistic data association (MC = 100).

TABLE 2. Track swap number for varied true and spoofed measurements.

	I / J	1	2	3	4	5	6
NN	4	3	7	28	29	74	79
	5	2	8	14	28	42	48
	6	0	0	4	7	31	33
PDA	4	1	2	9	21	43	61
	5	1	4	14	21	31	34
	6	0	0	3	7	19	22

true and spoofed follow the same path in the carry-off, the evolved M-best position estimates correspond to the same ground truth, and hence, we observe this raise in PRMSE as in Figs. 9, 10, and 11. The calculated weighted innovation, by considering the observations within the gating region is different from the actual innovation seen in the NN technique. However, in the deceiving interval, a degraded PRMSE is observed with PDA as compared to that of the NN technique. Due to the probabilistic decision during the deceiving period, the navigation track to follow spoof track decreases. In Table 2, the algorithm's TS is presented, where we can observe that the PDA outperforms NN even as the number of spoofed measurements injection increases. Furthermore, the overall computational load of the algorithm depends on the M-best positions and the total number of measurements being involved in the ILS. However, due to advancement in computational algorithms and hardware realizations, it is possible to achieve a high-speed processing hardware in a compact form.

2) URBAN ENVIRONMENT

If the available authentic measurements are greater than or equal to number of unknowns in the pseudomeasurement equation. Then unique solution exists and it is clearly depicted in the open space environment case in Section-V-C1.

To evaluate the urban environment, we assumed that the available authentic measurement set consists of four measurements, in which multi-path measurements are also present. The multi-path measurement usually differs from the actual

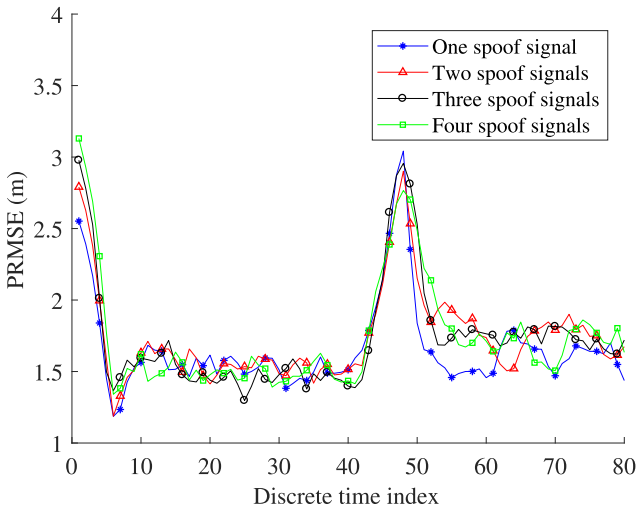

FIGURE 11. PRMSE for fixed six authentic signals and variable number of spoofed signal injections with probabilistic data association (MC=100).

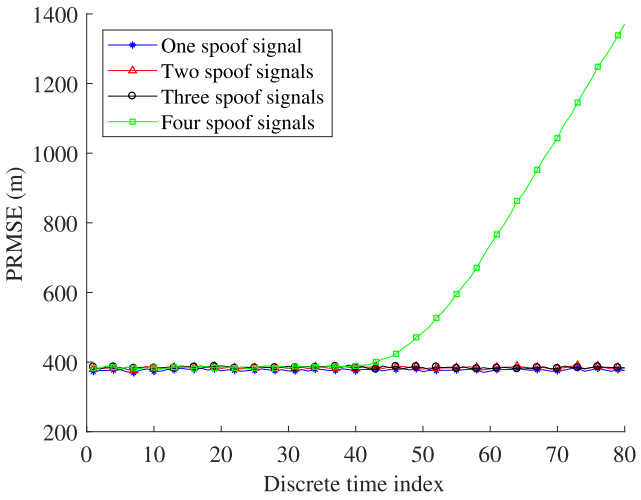

FIGURE 12. PRMSE for fixed four authentic measurements (three LOS measurements and one multi-path measurement) and variable number of spoofed measurement injections with nearest neighbour data association (MC=100).

measurement by the phase and distance between source and receiver. Since this paper dealt with the distance as a measurement to the estimator, the phase component is ignored. In the first case, one multi-path measurement exists and it is deflecting with 150 m range, whereas the rest of the three measurements are LOS to the receiver. The simulations are carried out for this case and the PRMSE is depicted in Fig. 12. In this case, we can observe that the M-best assignment solution of (25) is minimum for the authentic measurement set even though it contains one multi-path measurement. Here, out of four measurements, one multi-path measurement exist and as a result of that the PRMSE is increased to 380 m. We can observe that the cost minimization function is able to mitigate the effect of spoofing upto three spoof measurements. On the other hand, the M-best cost minimization of (25) provides the spoof location as the best location rather than the true

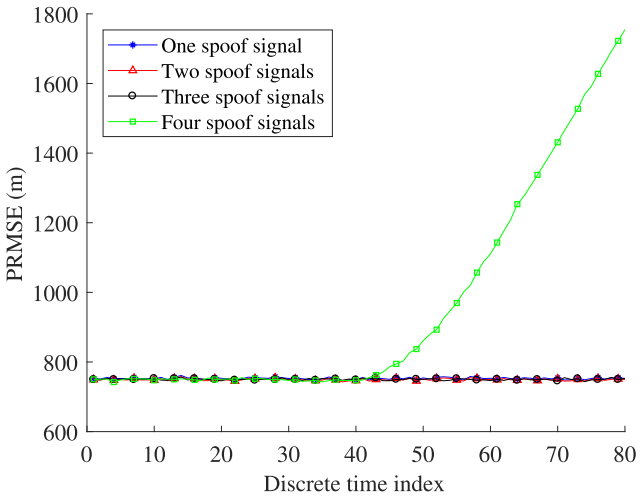

FIGURE 13. PRMSE for fixed four authentic measurements (two LOS measurements and two multi-path measurement) and variable number of spoofed measurement injections with nearest neighbour data association (MC=100).

location for the case of four spoof measurements, which is clearly shown in Fig. 12.

However, further investigation of multi-path effect in the spoofing environment, is performed with increased number of multi-path signals. In this case, out of four measurements in the authentic set, two LOS signals and two multi-path signals are considered. The multi-path measurements are deflected by 150 m and 250 m in range respectively, and PRMSE is plotted in Fig. 13. From the fig. 13, it is observed that the average PRMSE is raised to 750 m for the spoof injections of $J = 1, 2, \&3$. Whereas, for $J = 4$, the M-best cost minimization function of (25) is getting minimized for the spoof measurement set and eventually following the spoof trajectory. It is also observed that, in very few monto carlo runs, the measurement-to-track association is carried out for true rather than the spoof(only 7 runs out of 100 runs possess correct measurement-to-track association). Hence the TS is not tabulated for this special case.

From the results obtained, it is apparent that, the algorithm has a limitation to mitigate more than four spoof signals in the urban environment. Even though, the NN and PDA data associations are deployed, we observe insignificant improvement in the PRMSE value. There is a future scope to formulate a research problem by using the attributes of the signal (i.e., amplitude, phase, power) and solve the constrained optimization problem to address spoofing problem in urban scenario.

VI. CONCLUSION

This paper proposes an efficient alleviating method for GPS spoofing by using M-best likelihood-based optimization and a Kalman filter with data association. A novel technique of accepting all the authentic GPS signals and spoofed signals into the robust positioning algorithm, at every epoch, is presented in this paper. The robust positioning algorithm computes all possible combinations of pseudoranges, using the ILS solution. M-best position algorithm is successfully deployed to decrease the computational complexity of the robust positioning algorithm. To further accomplish the performance of the proposed method, Kalman filter followed by data association, is given and a lower track swapping rate with probabilistic data association is achieved. Simulations demonstrate that the proposed methodology is efficiently working for higher to lower satellite visibility, even with the increase in spoofed signal injections.

The future works can address the non-ideal spoofer scenario, selection of positioning algorithm for non-Gaussian measurement noise, development of navigation track for the non-Gaussian case, development of data association, and low computation algorithms. Furthermore, one can carry out the problem of spoofing effect mitigation in urban environment using the signal attributes and constrained optimization.

ACKNOWLEDGMENT

Bethi Pardhasaradhi would like to thank Prof. T. Kirubarajan and Dr. R. Tharmarasa for providing valuable inputs during the stay at ETF Laboratory, McMaster University, Canada, as a Visiting Research Scholar from 2018 to 2019.

REFERENCES

[1] B. W. Parkinson, P. Enge, P. Axelrad, and J. J. Spilker, Jr, *Global Positioning System: Theory and Applications*, vol. 2. Washington, DC, USA: American Institute of Aeronautics and Astronautics AIAA, 1996.

[2] J. Farrell and M. Barth, *The Global Positioning System and Inertial Navigation*, vol. 61. New York, NY, USA: McGraw-Hill, 1999.

[3] M. Wildemeersch, E. C. Pons, A. Rabbachin, and J. F. Guasch, "Impact study of unintentional interference on GNSS receivers," Eur. Commission, Joing Res. Centre, JRC Sci. Tech. Rep., 2010. [Online]. Available: https://publications.jrc.ec.europa.eu/repository/bitstream/JRC62607/ibna24742enc.pdf

[4] R. Schroer, "Electronic warfare. [A century of powered flight: 1903-2003]," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 18, no. 7, pp. 49–54, Jul. 2003.

[5] D. Schmidt, K. Radke, S. Camtepe, E. Foo, and M. Ren, "A survey and analysis of the GNSS spoofing threat and countermeasures," *ACM Comput. Surv.*, vol. 48, no. 4, p. 64, May 2016.

[6] N.-N. Zheng, S. Tang, H. Cheng, Q. Li, G. Lai, and F.-W. Wang, "Toward intelligent driver-assistance and safety warning system," *IEEE Intell. Syst.*, vol. 19, no. 2, pp. 8–11, Mar./Apr. 2004.

[7] J. P. F. Trovao, "An overview of automotive electronics," *IEEE Veh. Technol. Mag.*, vol. 14, pp. 130–137, 2019.

[8] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "GPS vulnerability to spoofing threats and a review of antispoofing techniques," *Int. J. Navigat. Observ.*, vol. 2012, Jul. 2012, Art. no. 127072.

[9] C. Günther, "A survey of spoofing and counter-measures: A survey of spoofing and counter-measures," *Navigation*, vol. 61, no. 3, pp. 159–177, Sep. 2014.

[10] M. L. Psiaki and T. E. Humphreys, "GNSS spoofing and detection," *Proc. IEEE*, vol. 104, no. 6, pp. 1258–1270, Jun. 2016.

[11] K. D. Wesson, J. N. Gross, T. E. Humphreys, and B. L. Evans, "GNSS signal authentication via power and distortion monitoring," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 54, no. 2, pp. 739–754, Apr. 2018.

[12] X. Fan, L. Du, and D. Duan, "Synchrophasor data correction under GPS spoofing attack: A state estimation-based approach," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4538–4546, Sep. 2018.

[13] E. G. Manfredini, "Signal processing techniques for GNSS anti-spoofing algorithms," Ph.D. dissertation, Dept. Electron. Eng., Politecnico di Tori, Turin, Italy, 2017.

[14] B. M. Ledvina, W. J. Bencze, B. Galusha, and I. Miller, "An in-line anti-spoofing module for legacy civil GPS receivers," in *Proc. Int. Tech. Meeting Inst. Navigat. (ION-ITM)*, San Diego, CA, USA, Jan. 2010, pp. 698–712.

[15] D. Miralles, A. Bornot, P. Rouquette, N. Levigne, D. M. Akos, Y.-H. Chen, S. Lo, and T. Walter, "An assessment of GPS spoofing detection via radio power and signal quality monitoring for aviation safety operations," *IEEE Intell. Transp. Syst. Mag.*, vol. 12, no. 3, pp. 136–146, Fall 2020.
[16] T. E. Humphreys, "Detection strategy for cryptographic GNSS anti-spoofing," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 49, no. 2, pp. 1073–1090, Apr. 2013.
[17] S. Tayeb, M. Pirouz, G. Esguerra, K. Ghobadi, J. Huang, R. Hill, D. Lawson, S. Li, T. Zhan, J. Zhan, and S. Latifi, "Securing the positioning signals of autonomous vehicles," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Dec. 2017, pp. 4522–4528.
[18] K. Wesson, M. Rothlisberger, and T. Humphreys, "Practical cryptographic civil GPS signal authentication," *J. Inst. Navigat.*, vol. 59, no. 3, pp. 177–193, Sep. 2012.
[19] M. L. Psiaki, B. W. O'Hanlon, J. A. Bhatti, D. P. Shepard, and T. E. Humphreys, "GPS spoofing detection via dual-receiver correlation of military signals," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 49, no. 4, pp. 2250–2267, Oct. 2014.
[20] C. H. Kang, S. Y. Kim, and C. G. Park, "Adaptive complex-EKF-based DOA estimation for GPS spoofing detection," *IET Signal Process.*, vol. 12, no. 2, pp. 174–181, Apr. 2018.
[21] F. A. Milaat and H. Liu, "Decentralized detection of GPS spoofing in vehicular ad hoc networks," *IEEE Commun. Lett.*, vol. 22, no. 6, pp. 1256–1259, Jun. 2018.
[22] Y. Liu, S. Li, Q. Fu, Z. Liu, and Q. Zhou, "Analysis of Kalman filter innovation-based GNSS spoofing detection method for INS/GNSS integrated navigation system," *IEEE Sensors J.*, vol. 19, no. 13, pp. 5167–5178, Jul. 2019.
[23] P. F. Swaszek, S. A. Pratz, B. N. Arocho, K. C. Seals, and R. J. Hartnett, "GNSS spoof detection using shipboard IMU measurements," in *Proc. 27th Int. Tech. Meeting Satell. Division Inst. Navigat. (ION GNSS)*, Tampa, FL, USA, Sep. 2014, pp. 745–758.
[24] M. Majidi, A. Erfanian, and H. Khaloozadeh, "Prediction-discrepancy based on innovative particle filter for estimating UAV true position in the presence of the GPS spoofing attacks," *IET Radar, Sonar Navigat.*, vol. 14, no. 6, pp. 887–897, Jun. 2020.
[25] D. Galar, U. Kumar, and D. Seneviratne, *Robots, Drones, UAVs and UGVs for Operation and Maintenance*. Boca Raton, FL, USA: CRC Press, 2020.
[26] Z. Ju, H. Zhang, and Y. Tan, "Distributed deception attack detection in platoon-based connected vehicle systems," *IEEE Trans. Veh. Technol.*, vol. 69, no. 5, pp. 4609–4620, May 2020.
[27] Y. Cui and S. S. Ge, "Autonomous vehicle positioning with GPS in urban canyon environments," *IEEE Trans. Robot. Autom.*, vol. 19, no. 1, pp. 15–25, Feb. 2003.
[28] K. Fallahi, C.-T. Cheng, and M. Fattouche, "Robust positioning systems in the presence of outliers under weak GPS signal conditions," *IEEE Syst. J.*, vol. 6, no. 3, pp. 401–413, Sep. 2012.
[29] T.-H. Chang, L.-S. Wang, and F.-R. Chang, "A solution to the ill-conditioned GPS positioning problem in an urban environment," *IEEE Trans. Intell. Transp. Syst.*, vol. 10, no. 1, pp. 135–145, Mar. 2009.
[30] Y. Oshman and M. Koifman, "Robust navigation using the global positioning system in the presence of spoofing," *J. Guid., Control, Dyn.*, vol. 29, no. 1, pp. 95–104, Jan. 2006.
[31] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Capkun, "On the requirements for successful GPS spoofing attacks," in *Proc. 18th ACM Conf. Comput. Commun. Secur. (CCS)*, 2011, pp. 75–86.
[32] M. Coulon, A. Chabory, A. Garcia-Pena, J. Vezinet, C. Macabiau, P. Estival, P. Ladoux, and B. Roturier, "Characterization of meaconing and its impact on GNSS receivers," in *Proc. 33rd Int. Tech. Meeting Satell. Division Inst. Navigat. (ION GNSS)*, 2020, pp. 3713–3737.
[33] D. Marnach, S. Mauw, M. Martins, and C. Harpes, "Detecting meaconing attacks by analysing the clock bias of GNSS receivers," *Artif. Satell.*, vol. 48, no. 2, pp. 63–83, Jan. 2013.
[34] A. Polydoros and C. Weber, "A unified approach to serial search spread-spectrum code acquisition—Part I: General theory," *IEEE Trans. Commun.*, vol. COM-32, no. 5, pp. 542–549, May 1984.
[35] A. Malyshev, I. Malay, and M. Ozerov, "Algorithm for separating GNSS signals into components," in *Proc. IEEE East-West Design Test Symp. (EWDTS)*, Sep. 2018, pp. 1–4.
[36] S. Deb, M. Yeddanapudi, K. Pattipati, and Y. Bar-Shalom, "A generalized S-D assignment algorithm for multisensor-multitarget state estimation," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 33, no. 2, pp. 523–538, Apr. 1997.
[37] M. L. Miller, H. S. Stone, and I. J. Cox, "Optimizing Murty's ranked assignment method," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 33, no. 3, pp. 851–862, Jul. 1997.
[38] R. Danchick and G. Newnam, "Reformulating Reid's MHT method with generalised Murty K-best ranked linear assignment algorithm," *IEE Proc.-Radar, Sonar Navigat.*, vol. 153, no. 1, pp. 13–22, 2006.
[39] P. Bethi, S. Pathipati, and P. Aparna, "Stealthy GPS spoofing: Spoofer systems, spoofing techniques and strategies," in *Proc. IEEE 17th India Council Int. Conf. (INDICON)*, Dec. 2020, pp. 1–7.
[40] C. Tanil, S. Khanafseh, M. Joerger, and B. Pervan, "An INS monitor to detect GNSS spoofers capable of tracking vehicle position," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 54, no. 1, pp. 131–143, Feb. 2018.
[41] Y. Bar-Shalom, P. K. Willett, and X. Tian, *Tracking Data Fusion*, vol. 11. Storrs, CT, USA: YBS, 2011.
[42] X. Lin, T. Kirubarajan, Y. Bar-Shalom, and X. Li, "Enhanced accuracy GPS navigation using the interacting multiple model estimator," in *Proc. IEEE Aerosp. Conf.*, vol. 4, Mar. 2001, pp. 4–19.

BETHI PARDHASARADHI (Member, IEEE) received the B.Tech. degree in electronics and communication engineering from Jawaharlal Nehru Technological University, Kakinada (JNTU-K), India, in 2014, and the M.Tech. degree in VLSI design from the Indian Institute of Information Technology and Management, Gwalior (IIITM), India, in 2016. He is currently pursuing the Ph.D. degree with the National Institute of Technology Karnataka (NIT-K), Surathkal, India. He was a Visiting Ph.D. Scholar with the ETF Laboratory, McMaster University, Canada, under the supervision of Prof. T. Kirubarajan from 2018 to 2019. His research interests include intentional interference in navigation, target tracking, and information fusion. He was a receipt of Sir C. V. Raman Award from the Institution of Engineering and Technology (IET) for outstanding academics and research.

PATHIPATI SRIHARI (Senior Member, IEEE) received the B.Tech. degree in electronics and communication engineering from Sri Venkateswara University, the master's degree in communications engineering and signal processing from the University of Plymouth, U.K., and the Ph.D. degree in radar signal processing from Andhra University, in 2012. He worked as a Visiting Assistant Professor with McMaster University, Canada, in 2014. He is currently working as an Assistant Professor with the National Institute of Technology Karnataka, Surathkal, India. His research interests include radar target tracking, radar waveform design, and efficient DSP algorithms for radar applications. He is also a member of IEICE, Japan, a Senior Member of ACM, and a Fellow of IETE. He received the 2010 IEEE Asia Pacific Outstanding Branch Counselor Award. He also received Young Scientist Award from the Department of Science and Technology (DST), New Delhi, to carryout sponsored research project entitled Development of efficient target tracking algorithms in the presence of ECM.

P. APARNA (Senior Member, IEEE) has been associated with NITK Surathkal since 2002 under various capacities. She has also been working as an Assistant Professor with NITK Surathkal since 2008. Her research interests include bio-medical signal processing, signal compression, computer architecture, and embedded systems. She has presented a number of research articles in various international conferences. She has conducted a number of workshops in the area of embedded systems and ARM processor. She has published more than 25 research articles in various journals and conference proceedings. She has guided two Ph.D. students and currently guiding five other research students. She is also working for two research and development projects, one of which is under SMDP-VLSI C2SD by Government of India and other is by LRDE, DRDO, India. She is actively involved in the research activities in the area of signal processing since ten years.