IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 25, 2022, accepted March 14, 2022, date of publication March 16, 2022, date of current version April 26, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3160047

GNSS Spoofing Detection and Mitigation in Multireceiver Configuration via Tracklets and Spoofer Localization

BETHI PARDHASARADHI[1], (Member, IEEE), GUNNERY SRINATH[1], (Graduate Student Member, IEEE), G. S. VANDANA[2], (Member, IEEE), PATHIPATI SRIHARI[1], (Senior Member, IEEE), AND P. APARNA[1], (Senior Member, IEEE)

[1]ECE Department, National Institute of Technology Karnataka, Surathkal, Surathkal 575025, India
[2]Sri Shasha Prayathi Technologies Private Ltd., Mangaluru 575025, India

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

ABSTRACT Global navigation satellite systems (GNSS) sensors estimate its position, velocity, and time (PVT) using pseudorange measurements. When there is no interference, the pseudoranges are due to authentic satellites, and the bearings is distinguishable. Whereas, in the presence of any intentional interference source like spoofer, the pseudorange measurements owing to spurious signals and all the bearings from the same direction. These spurious attacks yield either no position or falsified position to the GNSS receiver. This paper proposes to install multiple GNSS receivers on a vehicle (assumed to be cooperative) to detect and mitigate the spoofing attack. While installing multiple GNSS receivers, we assume that each GNSS receiver's relative position vector (RPV) is assumed to be known to other GNSS receivers. The installed GNSS receivers use the extended Kalman filter (EKF) framework to estimate their PVT. We proposed to calculate the equivalent-measurement and equivalent-measurement covariance of each GNSS receiver in the Cartesian coordinates in the tracklet framework. These tracklets are translated to the vehicle center using RPV to obtain translated-tracklets. The translated tracklet based generalized likelihood ratio test (GLRT) is derived to detect the spoofing attack at a given epoch. In addition to that, these translated-tracklets are processed in a batch least square (LS) framework to obtain the vehicle position. Once the attack is detected at a specific epoch, it quantifies that the position information is false. Moreover, another spoofing test is also formulated using DOA of signals. Once both the tests confirm the spoofing attack, the spoofer localization is performed using pseudo-updated states of GNSS receivers and acquired bearings in the iterative least-squares (ILS) framework. Mitigation of spoofing attack can be achieved either by projecting a null beam in the direction of the spoofer or by launching a counter-attack on the spoofer. The simulation results demonstrate that the proposed algorithm detects spoofing attacks and ensures continuity in the navigation track. As the number of satellite signals increases, the algorithms provide better position root mean square error (PRMSE) for GNSS receivers track, vehicle track, and spoofer localization.

INDEX TERMS GNSS intentional interference, spoofer localization, spoofing detection, GLRT, bearings only localization.

I. INTRODUCTION

Global navigation satellite systems (GNSS) are known for providing the position, velocity, and time (PVT) information across the globe for various civilian and military applications [1]. The GNSS received power is very low, making the receivers susceptible to various intentional and non-intentional interferences. The GNSS standards and blueprints are readily available in the market, making a wide range of attacks on the GNSS sensors [2]. The intensional interference sources are typically jammer, meaconer, and spoofer. Jammer is a device that transmits noise in the same frequency and makes the GNSS receiver fail to acquire the measurements [3]. Whereas, meaconer is a trans-receiver

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

device that stores the received authentic satellite signals and then transmits them onto the GNSS receiver at another time or place [4]. Moreover, the spoofer is a receive-analyze-transmit device that analyzes the time-varying dynamics of the GNSS receiver to alter the received authentic signals before re-transmission. The mimic GNSS signals produced by the spoofer yield to false positioning [5].

The direction of arrivals (DOAs) received by a GNSS receiver from the satellites is distinguishable for a clean environment. On the other hand, in an intentional interference case, either the spoofer or a jammer transmits the fake signals towards the GNSS receiver. Hence, all the DOAs are in the same direction of the spurious source [6], [7]. Adaptive complex-EKF-based DOA estimation is presented in [6] to detect the spoofing attack based on the fact that all spurious signals are in the same direction. Robust spoofing detection is proposed by estimating the DOA of signals, and a spatial null carries out mitigation in the array reception pattern [7]. During the spoofing attack and mitigation process, the GNSS receivers lack the PVT solution. Similar to the above contributions, multiple GNSS receivers-based spoofing detection is suggested in [8]–[10]. Multiple mobile COTS receivers are used to detect the spoofing effect is introduced in [8], where the optimal genie detector is derived based on the assumption that the true positions are perfectly known, and the observation errors are Gaussian. The differential pseudoranges are considered from multiple receivers to detect the spoofing [9] by exploiting the time difference of arrival (TDOA) properties between spoofing and authentic signals. In [9], it is assumed that the TDOAs of spoofing signals from a spoofer is identical. However, this assumption fails in the case of stealthy GPS spoofing by employing multiple spoofers to spoof multiple GNSS receivers [11]. In another communication, a differential pseudorange and carrier frequency measurements are used in a double antenna configuration to detect the spoofing attack [10]. Moreover, GNSS receivers with external range sensors are explored in [12] and detected the spoofing attack assuming only one GNSS receiver is in spoof attack and the rest are not being affected by spoofing. The spoofing attack detection is a primary mechanism to know whether the navigation is based on the authentic satellite signals or spurious signals [6]–[10], [12]. Even though the above literature successfully detect the spoofing attack, it lacks in estimating its PVT. Therefore, the navigation of GNSS is a significant research area of interest.

The spurious attack mitigation can be carryout by localizing the source or projecting the null beam in the direction of spurious signals. The TDOA method is explored in [9] to detect the spoofing effect and localize the source based on the fact that signals are coming from the same source possess exact time. Similarly, the localization of jammer is also addressed with the TDOA in [13]. The jamming localization problem is solved by rotating the un-manned air vehicle (UAV) at multiple fixed positions to get the antenna gain pattern and estimate the strength and bearings [14]. In addition, the received signal strength (RSS) measurements are used in networked receivers to localize the jammers [15]. Simultaneous localization of jammer and target with power difference of arrival (PDOA) and graph theory is jointly applied to accomplish desired performance [16]. Moreover, the meaconer localization problem is addressed with the help of space-time double-difference models [17]. Furthermore, the localization of spoofer using a large-scale air traffic surveillance system is presented in [18]. The localization of spoofer is also explored by using a vehicle-to-vehicle communication in [19]. While solving the spoofer localization in [13], [16], it was assumed that the GNSS receiver location was known and was not being influenced by the attack. However, in reality, the spoofing process implicates the fake position to the GNSS receiver, and hence the closed-form solution using the GNSS fake position results in false localization. Interestingly, the received bearings measurement depends on the estimated GNSS receiver location due to the arctan function.

In the above-cited papers [6]–[10], [12], a detection test is derived to distinguish the spoofing and non-spoofing activity. Further, all the earlier contributions were focused on spoofing detection. Hardly any research works are focused on navigation in the presence of spoofing. Therefore, we propose to install multiple GNSS receivers to detect and securely navigate the vehicle in a spoofing environment. Each GNSS receiver's relative position vector (RPV) pertaining to the vehicle center is assumed to be known precisely. The GNSS receivers estimate their state using the acquired pseudoranges in an extended Kalman filter framework. To calculate the vehicle position, we computed tracklets from the state estimates, such that its errors are not cross-correlated with the errors of any other data in the system. The tracklets are translated to a vehicle center using the RPV of each GNSS receiver, and the position is calculated using a batch least-squares solution. The estimated position of the vehicle is validated using a tracklets-based generalized likelihood ratio test (GLRT). Once the spoofing attack is detected, the mitigation of the effect should be followed. Hence, we propose to discard the updated state of the EKF at a given epoch and replace it with the pseudo-update state. This ensures the navigation of the vehicle in the spoofing environment.

The key contributions of the paper are

- This paper derived a compact mathematical model to generate the pseudorange measurements (true and false) for multiple GNSS receivers installed on a vehicle. This assumption is valid and implementable; for example, a vehicle like a car can accommodate four installations of GNSS receivers.
- We derived a tracklet framework for calculating each GNSS receiver's equivalent-measurement and equivalent-measurement covariance in the cartesian coordinate using the estimated GNSS states. This tracklet computation is based on the inverse Kalman filter approach and can be easily implemented in either hardware or firmware update. This method is more feasible in the cooperative model, and it does not

require any modifications to the existing GNSS receiver infrastructure.

- The vehicle's position is calculated based on the batch least squares using the translated-tracklets. The estimated position using Batch LS is validated using tracklets based generalized likelihood ratio test (GLRT). This test confirms whether the spoofing attack is carried out or not.
- Once the attack is detected at a given epoch, the updated state of the EKF at a given epoch is discarded and replaced with the pseudo-update state. This ensures the navigation solution of the GNSS in the spoofing environment. This pseudo-update state method is equally adaptable for the outlier pseudorange measurements, no-pseudorange measurements, and intentional pseudorange measurements case.
- Furthermore, the localization is also performed on the intentional interference source to mitigate the attack.

The rest of the paper is organized as follows. Section II states the problem formulation. In Section III, a generalized mathematical framework for multiple GNSS receivers in a spoofing environment is derived along with filtering and tracklets. Section IV explains the proposed methodology for spoofer attack detection and localization. Finally, results and conclusions are presented in Section V and Section VI.

II. PROBLEM FORMULATION

In a clean environment, a GNSS receiver located at $\mathbf{x}$ estimates its location as $\hat{\mathbf{x}}$, by using the authentic satellite set $\{\mathbf{x}_i\}_{i=1}^{M}$. Minimum of four visible satellites are required out of twenty four satellites present in constellation to estimate any unknown 3D location on the earth (example GPS). Let the problem be in 2D scenario, i.e., $\mathbf{x} = [x, y]'$ and $\mathbf{x}_i = [X_i, Y_i]'$. The bearings from M satellites is given by $\{\theta_i^t\}_{i=1}^{M}$ as shown in Fig. 1, where

$$\theta_i^t = \arctan\left(\frac{Y_i - y}{X_i - x}\right). \tag{1}$$

In a spoofing scenario, a spoofer is located at $\mathbf{x}^s$ and transmits spurious signals with higher power onto the GNSS receiver to create a fake location of $\mathbf{x}^f$. Once the GNSS receiver locked onto the spurious signals originated from the spoofer, the GNSS receiver estimates its location as $\mathbf{x}^f$ even though physically located at $\mathbf{x}$, as shown in Fig. 1. Where, $\mathbf{x}^s = [x^s, y^s]'$ and $\mathbf{x}^f = [x^f, y^f]$. The bearings corresponding to the spurious signals is $\left\{\theta_i^f\right\}_{i=1}^{M}$, and all spurious signals arrive in the same direction. The bearing measurements are given by

$$\theta_i^f = \arctan\left(\frac{y^s - y}{x^s - x}\right). \tag{2}$$

From (1) and (2), we can observe that the bearings is dependent on the physical state $\mathbf{x}$ and the source location $\mathbf{x}_i$ or $\mathbf{x}^s$. In a non-intentional interference case, in (1), the satellite locations are known since the received signal by the GPS receiver consists of the timestamp of signal transmission and

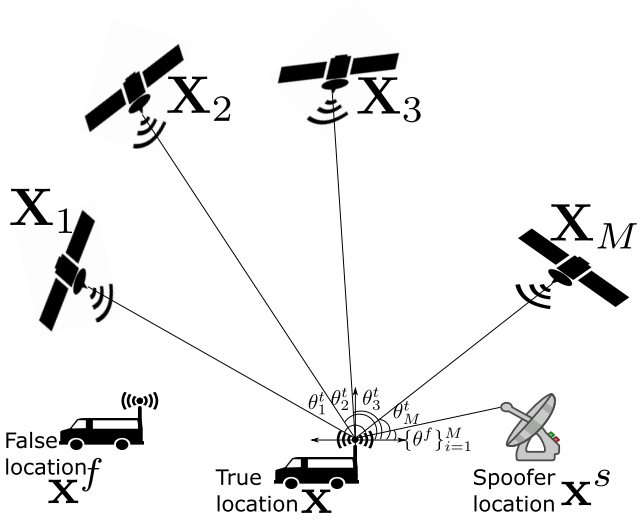

FIGURE 1. Spoofing scenario geometry and measurements.

satellite location information. Using multiple satellite signals, the GNSS receiver estimates its location as $\hat{\mathbf{x}}$. However, in (2), both the physical location of the GNSS receiver $\mathbf{x}$ and the spoofer location $\mathbf{x}^s$ are unknowns in the received bearings measurement. Interestingly, in spoofing activity, the position information related to the GNSS receiver is appeared to be $\mathbf{x}^f$ rather than $\mathbf{x}$. Hence, solving the bearings-only localization problem with multiple wrong positions of GNSS receivers results in an incorrect estimate of the source. Therefore, the following observations can be made.

- A generalized mathematical framework for spoofing effect on multiple GNSS receivers is to be derived.
- Once the spoofer attacks the GNSS receivers in the vicinity, there should be a mechanism to detect the spoofing attack using the estimated position from multiple GNSS receivers.
- Soon after the spoofing attack is detected, the false position $\mathbf{x}^f$ reported by the GNSS receiver at that discrete instant should be discarded, and need to establish an approximate physical location concerning to $\mathbf{x}$.
- Localization of the spoofer needs to be achieved using bearings information from multiple GNSS receivers and counter-attack the intentional interference source.

III. GNSS POSITIONING AND SPOOFING ATTACK DETECTION

This section provides the mathematical model for repeater-based spoofer and its influence on multiple GNSS receivers. Further, the equivalent-measurements calculation for the multiple GNSS receivers using tracklets is presented. After that, a GLRT is derived to detect the spoofing attack.

A. REPEATER BASED SPOOFER MEASUREMENTS

The GPS spoofing considered here is a repeater, in which the spoofer consists of a receiver, process unit, and transmitter module. The receiver module receives signals from the

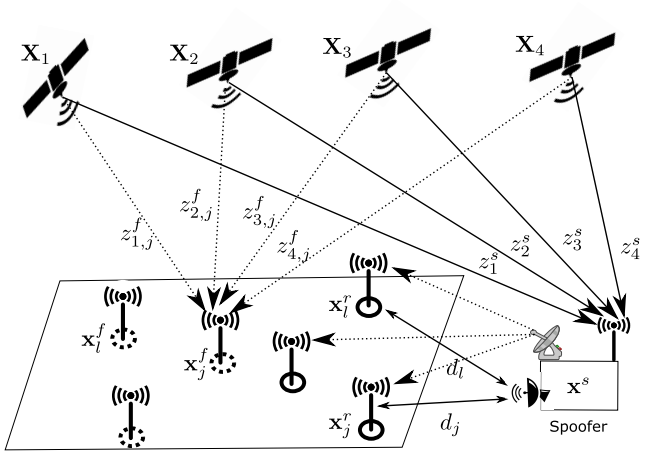

FIGURE 2. The geometry of a single spoofer multiple GNSS receiver spoofing scenario. The dark circle and the dotted circle represent the GNSS receiver's physical location and fake location, respectively. The dark lines and dotted lines represent the authentic pseudoranges and spoofer-generated (false) pseudoranges, respectively. The authentic pseudoranges for the vehicle are not drawn; however, they exist in reality.

authentic satellites, separated into different channels based on the satellite ID. A repeater-based spoofer system with analyzing capabilities is proposed in [20], in which the processing unit calculates the external delays for each satellite signal before re-transmission. Once the delays are added to the received authentic signals, the transmitter module transmits the spurious satellite signals S onto the targeted GNSS. The spoofer analyzes the vehicle's actual location (physical location), spoof location (wrong location intended to create) and accordingly calculates the delays to be incorporated. The spoofer is operating in escort/ stand-in mode to the vehicle to carry out stealthy spoofing. The spoofer intends to create a fake-position $\mathbf{x}_j^f$ for the vehicle j which is being physically located at $\mathbf{x}_j$ as shown in Fig. 2.

Here, N GNSS receivers are installed on the vehicle at $\{\mathbf{x}^r\}_{j=1}^N$ positions. In this process, not only GNSS receiver j gets into spoofed activity, but also all the GNSS receivers in the vicinity get into spoofing attack as stated in [21]. In Fig. 2, the dark lines from satellite-to-spoofer represent the reception of the original signal by the spoofer. These authentic satellite signals are captured by the spoofer located at $\mathbf{x}^s$, process and re-transmits onto GNSS receiver j located at $\mathbf{x}_j^r$ to create a fake location of $\mathbf{x}_j^f$. Since the spoofer is omnidirectional, the transmitted signal is receiving by all GNSS receivers within the vicinity of the spoofer. The spoofers use boosted power compared to the authentic satellite signals. Hence all the GNSS receivers get into spoof activity. Therefore, we can observe that three spoof locations corresponding to three GNSS receivers are as depicted in Fig. 2.

The spoofer located at $\mathbf{x}^s$ receives the authentic combined signal from all satellites in the range as

$$S\left(\mathbf{x}^s, t'\right) = \sum_{i=1}^{M} A_i S_i\left(t - \delta_i^s\right) + n\left(\mathbf{x}^s, t'\right), \tag{3}$$

where A_i is signal attenuation due to transmission from $\mathbf{x}_i$ to $\mathbf{x}^s$. Whereas t' is the global satellite time or system time, δ_i^s is the time-delay corresponding to the pseudorange measurement z_i^s. Spoofer modifies the time delays of individual satellite signals, then re-transmitted signal onto GNSS receiver j is represented as

$$S\left(\mathbf{x}^s, t'\right) = \sum_{i=1}^{M} A_i S_i\left(t - \delta_i^s - \delta_{i,j}\right) + n\left(\mathbf{x}^s, t'\right). \tag{4}$$

The external time delay offered to the i^{th} satellite signal by the spoofer for GNSS receiver j is given by $\delta_{i,j}$. The external delay calculation [22], [23] is given by

$$\delta_{i,j} = \frac{z_{i,j}^f - z_i^s - d_j}{c}. \tag{5}$$

The spoofer-to-GNSS receiver distance for j is d_j. In practice, range measuring devices and trackers are employed for the distance calculation [23]. To simplify the problem, we assumed that the distance between the spoofer and GNSS receiver was known precisely to the spoofer.

The re-transmitted signals propagate with velocity of light (c) in open space and are then received by the GNSS receiver. As shown in Fig. 2, the GNSS receiver located at $\mathbf{x}_l$ receives the combined signal as

$$S\left(\mathbf{x}_l, t'\right) = \sum_{i=1}^{M} A_{i,l} S_{i,l}\left(t - \delta_{i,l}^s - \delta_{i,j} - \frac{d_l}{c}\right) + n\left(\mathbf{x}_l, t'\right). \tag{6}$$

Here, $l \in \{1, \ldots, N\}$. For $l = j$, the above equation defines that all the signals transmitted by the spoofer are locking onto the GNSS receiver j. Whereas for $l \neq j$, the signals transmitted by spoofer are locking onto l^{th} GNSS receiver even though the spurious signals are generated for GNSS receiver j. After processing the received signals, the pseudorange measurements obtained are given by

$$z_{i,l}^s = c\left(\delta_i^s + \delta_{i,j} + \frac{d_l^s}{c}\right). \tag{7}$$

Substituting $\delta_i^s = \frac{z_i^s}{c}$ and (5) in (7) yields

$$z_{i,l}^s = c\left(\frac{z_i^s}{c} + \frac{z_{i,j}^f - z_i^s - d_j^s}{c} + \frac{d_l^s}{c}\right). \tag{8}$$

On simplifying the (8), we get

$$z_{i,l}^s = z_{i,j}^f - d_j^s + d_l^s. \tag{9}$$

The representation in (9) is the compact form to generate GPS measurements for single-spoofer multiple GNSS receivers spoofing case. In spoofing process, the pseudorange measurement set obtained at the GNSS receiver l due to spoofer is $\left\{z_{i,l}^f\right\}_{i=1}^M = \{z_i\}_{i=1}^M$. Here, we are ignoring the index of the GNSS receiver j to avoid the ambiguity in equations. Whereas in non-spoofing case, the pseudorange measurement set obtained for the GNSS receiver j is $\left\{z_i^r\right\}_{i=1}^M = \{z_i\}_{i=1}^M$.

B. EKF FOR GNSS RECEIVER POSITIONING

The pseudo measurement for GNSS receiver j is given by

$$\begin{aligned} z_{i,j} &= \rho_{i,j} + c\Delta t + w_{i,j} \\ &= \psi_{i,j} + w_{i,j}. \end{aligned} \tag{10}$$

where $\rho_{i,j}$ is the true range or geometrical range from satellite $\mathbf{x}_i$ to GNSS receiver located at $\mathbf{x}_j$, which is equal to $\sqrt{(X_i - x_j^r)^2 + (Y_i - y_j^r)^2}$. Where $c\Delta t$ and $w_{i,j}$ are bias due to offset and pseudorange measurement error for satellite i respectively. The measurement noise follows the white Gaussian noise with mean zero and variance σ. The stacking of M pseudorange measurements gives

$$\begin{aligned} z_j(k) &= \psi_j[X_j(k)] + w_j(k) \\ &= H(k)X_j(k) + w_j(k), \end{aligned} \tag{11}$$

where

$$\begin{aligned} z_j(k) &= \left[z_{1,j}(k), \cdots, z_{M,j}(k)\right]' \\ \psi_j(k) &= \left[\psi_{1,j}, \cdots, \psi_{M,j}\right]' \\ w_j(k) &= \left[w_{1,j}, \cdots, w_{M,j}\right]', \end{aligned}$$

and $H(k)$ is the linearized measurement transition matrix represented as

$$H = \frac{\partial \psi_j}{\partial \mathbf{x}_j} \Big|_{\mathbf{x}_j = \hat{\mathbf{x}}_j} = \begin{bmatrix} -h_1^x & 0 & -h_1^y & 0 & c \\ \vdots & 0 & \vdots & 0 & c \\ -h_M^x & 0 & -h_M^y & 0 & c \end{bmatrix}, \tag{12}$$

and the state is $X_j = [x_j, \dot{x}_j, y_j, \dot{y}_j, \delta t]$. Here

$$h_i^x = -\frac{\partial \psi_{i,j}}{\partial x} = \frac{(X_i - x)}{\sqrt{(X_i - x)^2 + (Y_i - y)^2}}.$$

$$h_i^y = -\frac{\partial \psi_{i,j}}{\partial y} = \frac{(Y_i - y)}{\sqrt{(X_i - x)^2 + (Y_i - y)^2}}.$$

The filter relaying on pseudo measurements at k and its last updates($\hat{\mathbf{x}}_i(k'|k')$ and $\hat{\mathbf{P}}_i(k'|k')$) to estimate state and covariance update at k. Here k' is the last epoch or last updated time. Hence, the vehicle state dynamics is

$$X_j(k) = F_j(k')X_j(k') + p_j(k'), \tag{13}$$

where $F_j(k')$ is the state transition matrix and $p_j(k')$ is process noise, follows zero mean additive WGN with covariance $Q_j(k')$. The predicted state and its associated covariance of the Kalman filter are

$$\hat{X}_j(k|k') = F_j(k')\hat{X}_j(k'|k'), \tag{14}$$

and

$$\hat{\mathbf{P}}_j(k|k') = F_j(k')\hat{\mathbf{P}}_j(k'|k')F_j(k')' + Q_j(k') \tag{15}$$

respectively. The measurement prediction is given by

$$\hat{z}_j(k|k') = H(k)\hat{X}_i(k|k'). \tag{16}$$

The residual and residual covariance are

$$r_j(k|k') = z_j(k) - \hat{z}_j(k|k'), \tag{17}$$

and

$$S_j(k) = H(k)\hat{\mathbf{P}}_j(k|k')H(k)' + R_j(k) \tag{18}$$

respectively. Here $R_j(k)$ is the measurement covariance matrix corresponding to the $z_j(k)$. The filter gain is given by

$$G_j(k) = \mathbf{P}_j(k|k')H(k)'S_j(k)^{-1}. \tag{19}$$

The updated state and its associated covariance are designated as

$$\hat{X}_j(k|k) = \hat{X}_j(k|k') + G_j(k)r_j(k), \tag{20}$$

and

$$\hat{\mathbf{P}}_j(k|k) = \hat{\mathbf{P}}_j(k|k') - G_j(k)S_j(k)G_j(k)' \tag{21}$$

respectively. Here, the measurements fed to the filter are pseudoranges. The state is a stacked vector of position and velocity. We are constructing the equivalent measurements in Cartesian space using the updated and predicted states of the filter.

C. TRACKLET COMPUTATION

A tracklet is a track computed so that its errors are not cross-correlated with the errors of any other data in the system for the same target [24]. A tracklet is like a large measurement (considers the position and velocity of the GNSS receiver). The tracklet based method provides approximate equivalent measurements of the reported tracks without additional assumptions. Moreover, it is not mandatory to have synchronous updates from all the filters. Tracklets can be computed between any two updates from the same GNSS receiver using inverse information filter, inverse Kalman filter, and measurement matrix [24]. Out of them, the inverse Kalman filter is easy to realize, and it only requires data from any two timestamps to compute tracklet at the required time stamp [25]. Here, the inverse Kalman filter-based tracklet computation method is applied. Inverse filtering is to infer the parameters of a filtering system by observing its output. This inverse filtering gained popularity in system identification, fault detection, image deblurring, and signal deconvolution. Based on this method, the equivalent measurement for GNSS receiver j using the filtered output at k' and k is $m_j(k, k')$. The timestamp information at these two instants should be available to compute equivalent measurements at a given epoch. Therefore, the equivalent measurement is as given in [25]

$$m_j(k, k') = \hat{X}_j(k|k') + A_j(k|k')\left[\hat{X}_j(k|k) - \hat{X}_j(k|k')\right], \tag{22}$$

where

$$m_j(k, k') = X_j(k) + \tilde{m}_j(k, k) \tag{23}$$

and

$$\mathbb{E}\left[\tilde{m}_j(k, k) \mid \mathbf{Z}_j^{k'}\right] = 0. \tag{24}$$

where $\mathbb{E}[\cdot]$ is an expectation operator. Here $\mathbf{Z}^{k'}$ represents the measurements upto k' time instant, that is

$\mathbf{Z}^{k'} = \{z_j(1), \cdots, z_j(k')\}$. The equivalent measurement error covariance matrix corresponding to $m_j(k, k')$ is $M_j(k, k')$ designated as

$$M_j(k, k') = \left[A_j(k|k') - \mathbf{I}\right] \mathbf{P}_j(k, k'). \tag{25}$$

Here, $\mathbf{I}$ is the identity matrix, and

$$A_j(k, k') = \mathbf{P}_j(k, k') \left[\mathbf{P}_j(k, k') - \mathbf{P}_j(k, k)\right]^{-1}. \tag{26}$$

Only the final equation of the equivalent measurement covariance is presented in (25), the detailed derivation is presented in APPENDIX. To compute tracklet at any discrete time instant k, one should have $\hat{X}_j(k|k)$, $\mathbf{P}_j(k, k)$, $\hat{X}_j(k'|k')$ and $\mathbf{P}_j(k', k')$. The tracklets can be computed for any number of lags. Because of this feasibility, if the filter update rate is different, it will not create any issues in the algorithm. However, to compute tracklet at k, the matrix $\left[\mathbf{P}_j(k, k') - \mathbf{P}_j(k, k)\right]$ has to be non-singular. The detailed derivation of the tracklet, its sub-optimality conditions, and non-singularity issues are presented in [26]. The equivalent measurement corresponding to the position of the GNSS receiver is represented as

$$z_{\mathbf{x}_j}(k) = \mathbb{F} m_j(k, k'), \tag{27}$$

where $\mathbb{F} = \text{diag}\{1, 0, 1, 0, 0\}$. Similar to that of state, the equivalent measurement covariance is given by

$$R_{\mathbf{x}_j}(k) = \mathbb{F} M_j(k, k') \mathbb{F}'. \tag{28}$$

Here, $\mathbb{F}$ is to extract the position information from the equivalent measurement vector. It is worth noting that the state vector and the equivalent measurement vector are of the same dimensions.

D. VEHICLE POSITIONING

We consider N GNSS receivers spatially deployed at $\{\mathbf{x}_j\}_{j=1}^{N}$ on a given vehicle as shown in Fig. 3. The location of the vehicle's centre is $\mathbf{x}$, which can be any arbitrary location (GNSS receiver is not necessarily present in that location). Since the installation of GNSS receivers is predefined, one can define the location of the GNSS receivers relative to the centre of the vehicle as illustrated in Fig. 3. Here, δ_j^x and δ_j^y are the relative distances of $\mathbf{x}_j$ with respect to $\mathbf{x}$. The relation between relative distance-vector, installed GNSS receivers location, and centre of the vehicle is given by

$$\mathbf{x} = \mathbf{x}_j + \begin{bmatrix} \delta x_j \\ \delta y_j \end{bmatrix}. \tag{29}$$

The equivalent measurement obtained for the GNSS receivers j is

$$z_{\mathbf{x}_j} = H_j \mathbf{x}_j + w_j, \tag{30}$$

where $H_j = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and w_j follows zero mean white Gaussian noise with covariance equal to $R_{\mathbf{x}_j}$. The measurements are translated with respect to the centre of the vehicle using the relative position vector, which is readily available. The modified measurements are designated as

$$z^t_{\mathbf{x}_j} = H_j \mathbf{x}_j + H_j \begin{bmatrix} \delta x_j \\ \delta y_j \end{bmatrix} + w_j \tag{31}$$

$$= H_j \mathbf{x} + w_j. \tag{32}$$

The (32) is obtained by substituting the (29) in (31). Considering all the N measurements, a batch least squares solution is formed to estimate the $\mathbf{x}$. The measurement transition matrix and the measurement noise covariance matrix for batch LS is given by

$$H^N = \begin{bmatrix} H_1 \\ \vdots \\ H_N \end{bmatrix}, \quad R^N = \text{diag}(R_{\mathbf{x}_1}, \cdots, R_{\mathbf{x}_N}). \tag{33}$$

The LS estimate is given by [27] as

$$\hat{\mathbf{x}} = \left[\left(H^N\right)' \left(R^N\right)^{-1} \left(H^N\right)\right]^{-1} \left(H^N\right)' \left(R^N\right)^{-1} \left(z^t_{\mathbf{x}_j}\right)^N \tag{34}$$

Substituting the (33) in (34) provides

$$\hat{\mathbf{x}} = \frac{1}{N} \sum_{j=1}^{N} z^t_{\mathbf{x}_j} \tag{35}$$

The above result in (35) using batch LS is equal to the sample mean of all the N observations.

In the given environment, a spoofer is located at $\mathbf{x}^s$ and trying to spoof any one of the GNSS receivers installed on the vehicle. In a crowded GNSS receivers case, the influence of spoofing is not limited to one receiver, and it corrupts all the position information of GNSS receivers in the vicinity [21]. Besides, due to the spoofing activity of the spoofer, GNSS receiver j is spoofed by a distance of $\Delta\mathbf{x}_j$. Where $\Delta\mathbf{x}_j = [\Delta x, \Delta y]'$. The relation between relative distance-vector, installed GNSS receiver location, and spoofed distance is given by

$$\mathbf{x} = \mathbf{x}_j + \Delta\mathbf{x}_j + \begin{bmatrix} \delta x_j \\ \delta y_j \end{bmatrix}. \tag{36}$$

The translated measurement for the GNSS receiver j using the relative distance vector is represented as

$$z^f_{\mathbf{x}_j} = H_j \mathbf{x}_j + \Delta\mathbf{x}_j + \begin{bmatrix} \delta x_j \\ \delta y_j \end{bmatrix} + w_j. \tag{37}$$

Here, the (37) contain two unknown vectors $\mathbf{x}_j$ and $\Delta\mathbf{x}_j$. The (37) is subjected to the batch LS framework as shown in the clean environment, and the estimate is given by

$$\hat{\mathbf{x}}^f = \frac{1}{N} \sum_{j=1}^{N} z^f_{\mathbf{x}_j} \tag{38}$$

By observing the (35) and (38), we can infer that the objectives of the proposed investigation is to detect the spoofing attack.

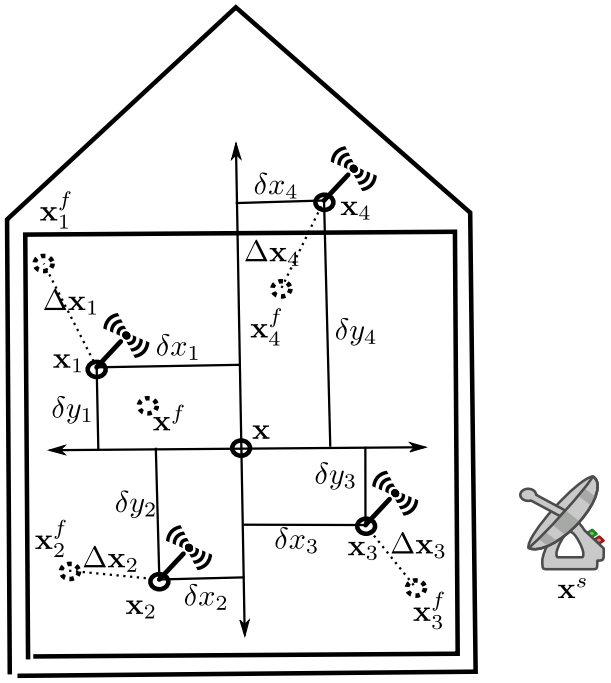

FIGURE 3. The geometry of multiple GNSS receivers installation on a vehicle (ship). The dark circle represents the actual position of the GNSS receiver, and the dotted circle represents the false position of the GNSS receiver in spoofing activity.

E. DETECTION OF A SPOOFING ATTACK WITH TRACKLETS

To detect the spoofing effect, we are establishing a binary hypothesis test using the obtained translated-tracklets. In no spoofing case, the hypothesis $\mathcal{H}_0$ is assuming that estimated positions of the GNSS receivers are owing to authentic measurements. Whereas, the hypothesis $\mathcal{H}_1$ is for the spoofing case, in which the estimated position estimates are false due to the spoofing. That is

$$\mathcal{H}_0 : z_{\mathbf{x}_j} = \mathbf{x}_j + \begin{bmatrix}\delta x_i \\ \delta y_i\end{bmatrix} + w_j; \quad j = 1, \cdots, N \tag{39}$$

$$\mathcal{H}_1 : z_{\mathbf{x}_j} = \mathbf{x}_j + \Delta\mathbf{x}_j + \begin{bmatrix}\delta x_i \\ \delta y_i\end{bmatrix} + w_j; \quad j = 1, \cdots, N \tag{40}$$

The observations in (39) and (40) follow a normal distribution and the noise samples are independent of each other. The pdf of likelihood of observations under the given hypothesis $\mathcal{H}_0$ is

$$p\left(z_{\mathbf{x}_j}; \mathbf{x}_j, \begin{bmatrix}\delta x_i \\ \delta y_i\end{bmatrix}, \mathcal{H}_0\right) = \prod_{j=1}^{N} p\left(z_{\mathbf{x}_j}^t \mid \mathbf{x}\right). \tag{41}$$

Similarly, the pdf of likelihood of observations under the given hypothesis $\mathcal{H}_1$ is

$$p\left(z_{\mathbf{x}_j}; \mathbf{x}_j, \begin{bmatrix}\delta x_i \\ \delta y_i\end{bmatrix}, \Delta\mathbf{x}_j, \mathcal{H}_1\right) = \prod_{j=1}^{N} p\left(z_{\mathbf{x}_j}^f \mid \mathbf{x}\right). \tag{42}$$

The generalized likelihood ratio test (GLRT) of the above two hypothesis is given by

$$\frac{p\left(z_{\mathbf{x}_j}; \mathbf{x}_j, \begin{bmatrix}\delta x_i \\ \delta y_i\end{bmatrix}, \Delta\mathbf{x}_j, \mathcal{H}_1\right)}{p\left(z_{\mathbf{x}_j}; \mathbf{x}_j, \begin{bmatrix}\delta x_i \\ \delta y_i\end{bmatrix}, \mathcal{H}_0\right)} = \frac{\prod_{j=1}^{N} p\left(z_{\mathbf{x}_j}^f \mid \mathbf{x}\right)}{\prod_{j=1}^{N} p\left(z_{\mathbf{x}_j}^t \mid \mathbf{x}\right)} \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \gamma \tag{43}$$

At time index k, the GLRT [28] is evaluated to distinguish between a spoofing attack is present or not. If the GLRT is greater than the threshold γ, the flag signal $\zeta = 1$, then it indicates the presence of spoofing attack; else $\zeta = 0$, there is no spoofing attack. Therefore

$$\zeta(k) = \begin{cases} 1; & \text{spoofing attack presence} \\ 0; & \text{no spoofing attack.} \end{cases} \tag{44}$$

F. SPOOFING ATTACK DETECTION WITH BEARINGS

Along with the GLRT spoofing detection test (in Section III-E), another spoofing attack detection is also considering by using the bearings. In a clean environment, all the bearings $\{\theta_i^t\}_{i=1}^M$ are distinguishable, since the bearings are from different source locations (different satellites). Whereas in spoofing attack, the bearings $\{\theta_i^f\}_{i=1}^M$ are in-distinguishable since all the bearings from same direction of the spoofer [6]. Therefore at time k, the detector gives

$$\eta(k) = \begin{cases} 0; & \theta_i \neq \theta_j \quad \forall \quad i, j = 1, 2, \ldots M \quad \text{where} \quad i \neq j \\ 1; & \text{else} \end{cases} \tag{45}$$

Here, η is a flag signal to distinguish the spoofing attack or not.

IV. PSEUDO-TRACK AND SPOOFER LOCALIZATION

Once the spoofing attack is confirmed using the GLRT and bearings test, the spoofer localization is essential to mitigate the spoofing effect. However, during the spoofing attack, the position integrity of the GNSS receivers is not preserving. Hence, we propose a pseudo-track updation [29] technique to approximately calculate the vehicle and GNSS sensors position.

A. PSEUDO TRACK OF THE VEHICLE

At discrete time index k, the spoofer attack is detected by using the GLRT and bearings. Hence, the estimated position at k using batch LS results in $\hat{\mathbf{x}}^f(k)$ rather than $\hat{\mathbf{x}}(k)$. Therefore, an approximate position of the GNSS location is required to perform localization using bearings-only information. The updated position can be approximated by using the pseudo-position method given in [29]. At k, the failure of measurement (spoofing) or unavailability of measurement (jamming) results in a lack of updated state at k^{th} instant. However, one can assume the updated state as predicted state in the intentional interference case as suggested in [27], [29]

$$X_j(k) = F_j(k')\hat{X}_j(k') \tag{46}$$

B. SOURCE LOCALIZATION WITH BEARINGS

The source localization is performed at a given k using the pseudo-position of GNSS receivers and observed bearings. The spoofer is located at $\mathbf{x}^s$ and transmitting the spurious signals onto the vehicle. The localization problem can be formulated as LS, ILS, and newtons methods [30]. However, the ILS outperforms other methods. Hence, we are formulating the ILS to localize the spoofing source; since this method iteratively improves the current estimate using the measurements until accomplishes the desired accuracy.

The measurement model for the bearings corresponding to the GNSS receiver j is

$$\begin{aligned}\theta_j &= h\left(\mathbf{x}^s, \mathbf{x}_j\right) + v_j \\ &= \arctan\left(\frac{y^s - y_j}{x^s - x_j}\right) + v_j; \quad j = 1, \cdots, N \end{aligned} \tag{47}$$

where v_j is the zero mean white Gaussian measurement noise with variance σ_θ^2. In (47), x_j and y_j are the pseudo-positions obtained by using the prediction of the previous state. It is worth to look at the difference between (2) and (47). Where, (2) involves with the false position of the GNSS receiver, and (47) is function of pseudo-update position of the GNSS receiver. The stacked vector Θ of all the available bearings is given by

$$\begin{aligned}\Theta &= \begin{bmatrix}\theta_1 \\ \vdots \\ \theta_N\end{bmatrix} \\ &= \mathbf{h}\left(\mathbf{x}^s, \mathbf{x}_j\right) + \mathbf{v}\end{aligned} \tag{48}$$

where

$$\mathbf{h}(\mathbf{x}^s) = \begin{bmatrix} h\left(\mathbf{x}^s, \mathbf{x}_1\right) \\ \vdots \\ h\left(\mathbf{x}^s, \mathbf{x}_N\right)\end{bmatrix}, \quad \mathbf{v} = \begin{bmatrix} v_1 \\ \vdots \\ v_N\end{bmatrix} \tag{49}$$

Using the estimate $\hat{\mathbf{x}}_n^s$ at the end of iteration n, one can update the ILS estimate as $\hat{\mathbf{x}}_{n+1}^s$ using [27]

$$\hat{\mathbf{x}}_{n+1}^s = \hat{\mathbf{x}}_n^s + \left(J_n' \mathcal{R}^{-1} J_n\right)^{-1} J_n' \mathcal{R}^{-1} \left[\Theta - \mathbf{h}\left(\hat{\mathbf{x}}_n^s, \mathbf{x}_j\right)\right] \tag{50}$$

where J_n is the Jacobian matrix represented as

$$J_n = \begin{bmatrix} \dfrac{\partial h\left(x^s, x_1\right)}{\partial x} & \dfrac{\partial h\left(x^s, x_1\right)}{\partial y} \\ \vdots & \vdots \\ \dfrac{\partial h\left(x^s, x_N\right)}{\partial x} & \dfrac{\partial h\left(x^s, x_N\right)}{\partial y}\end{bmatrix}_{x^s = \hat{x}_n^s} \tag{51}$$

with

$$\begin{aligned}\frac{\partial h\left(x^s, x_j\right)}{\partial x^s} &= -\frac{y^s - y_j}{\left(x^s - x_j\right)^2 + \left(y^s - y_j\right)^2} \\ \frac{\partial h\left(x^s, x_j\right)}{\partial y^s} &= \frac{x^s - x_j}{\left(x^s - x_j\right)^2 + \left(y^s - y_j\right)^2}\end{aligned}$$

Convergence criteria is decided with the number of iterations or the achievable accuracy. Moreover, the initialization of the position is done by taking any two intersections from the given bearings only measurements.

C. SPOOFING MITIGATION

In spoofing activity, all the spoof signals are arriving in the same direction. Hence, by placing a null beam in the direction of source mitigates the spoofing [31]. However, to steer the null beam in that direction, one need to calculate the spoofer location and which is being carried out by using bearings information. When ever the flags ζ and η sets to one, it confirms spoofing activity and it enables the flag f, which is given by

$$f(k) = \begin{cases} 1; & (\zeta(k) == 1)\&\&(\eta(k) == 1) \\ 0; & \text{else.}\end{cases} \tag{52}$$

However, the flag $f(k)$ sometimes can be a false positive. Hence, we formulated a management module to study the flags over the time, which is similar to track management in target tracking applications [32]. We adopted m/n rule to make a decision about spoofing. In a given n scans of data, if flags are unity for m scans, it confirms spoofing activity. The quantifying metric to launch counter-measure against the spoofing activity is given from a decision metric

$$f_n = \sum_{i=0}^{n} f(k-i), \tag{53}$$

whenever this metric $f_n > m$, then the counter measure launches. This mitigation is possible by launching a counter-attack like null beam projection in the direction of spoofer or shooting the spoofer as a anti-spoofing measure as in defense applications. The overall algorithm flow corresponding to spoofing detection and mitigation is given in Algorithm 1.

V. RESULTS AND DISCUSSIONS

A. SIMULATION SCENARIO

WGS-84 with circular orbit assumption is used to simulate the satellite trajectories in both spoofing and non-spoofing cases. The positions of the satellite are given by

$$\begin{aligned}X(t) &= D\left[\cos\Omega(t)\ \cos\Phi(t) - \sin\Omega(t)\ \sin\Phi(t)\cos 55^\circ\right] \\ Y(t) &= D\left[\cos\Omega(t)\ \sin\Phi(t) + \sin\Omega(t)\ \cos\Phi(t)\cos 55^\circ\right]\end{aligned}$$

Here, $D = 26,560$ Km is the radius of the earth. whereas, Ω is the angular phase, and Φ is the right ascension in the circular orbit given by

$$\begin{aligned}\Omega(t) &= \Omega(0) - (t - t(0))\left(\frac{360}{86164}\right)^\circ \\ \Phi(t) &= \Phi(0) + (t - t(0))\left(\frac{360}{43082}\right)^\circ\end{aligned}$$

The satellites initial positions $t(0)$ are given in Table 1.

Superyachts to mega yachts usually vary from 24 m long to 100 m long. Hence we consider a yacht in our simulation

Algorithm 1 Algorithm Overview for GNSS Spoofing Detection and Mitigation

procedure Detection and Mitigation
  for $k = 1 :$ scans **do**
    for $j = 1 : M$ **do**
      Compute updated state $\hat{X}_j(k|k)$ and updated covariance $\hat{\mathbf{P}}_j(k|k)$ by using pseudorange measurements $\{z_{i,j}\}_{i=1}^{N}$. ▷ EKF framework
      Compute equivalent measurement $z_{\mathbf{x}_j}(k)$ and equivalent measurement covariance $R_{\mathbf{x}_j}$ by using prediction $\hat{X}_j(k|k')$, $\hat{\mathbf{P}}_j(k|k')$ and updated information $\hat{X}_j(k|k)$, $\hat{\mathbf{P}}_j(k|k)$. ▷ Tracklet framework
      Compute translated equivalent measurement $z^t_{\mathbf{x}_j}(k)$ by using equivalent measurement $z_{\mathbf{x}_j}(k)$ and RPV δx_j, δy_j. ▷ Translation
    end for
    Compute ζ by using translated equivalent measurement $z^t_{\mathbf{x}_j}(k)$. ▷ Spoofing test with tracklets
    Compute η by using the bearings information Θ. ▷ Spoofing test with Bearings
    if $(\zeta == 1)\&\&(\eta == 1)$ **then**
      for $j = 1 : M$ **do**
        Compute pseudo track update $\hat{X}^p_j(k|k)$ using predicted states $\hat{X}_j(k \mid k')$, $\hat{X}_j(k' \mid k'')$ and updated state $\hat{X}_j(k'|k')$. ▷ Pseudo track updation
      end for
      Compute centre of the vehicle $\hat{\mathbf{x}}(k)$ by using pseudo track updates $\left\{\hat{X}^p_j(k|k)\right\}_{j=1}^{M}$ ▷ batch LS framework
      Set flag $f(k) = 1$
      Compute spoofer state $\mathbf{x}^s$ using $\Theta(k)$ ▷ ILS framework
    else
      Compute vehicle location $\hat{\mathbf{x}}(k)$ using updated states $\left\{\hat{X}_j(k|k)\right\}_{j=1}^{M}$ ▷ batch LS framework
    end if
    Compute $f_{\sum}$ ▷ Windowing
    if $f_n > 3$ **then**
      Null beam projection towards $\mathbf{x}^s$ ▷ Spoofing mitigation
    end if
  end for
end procedure

scenario on which four GNSS receivers are installed. The yacht's center is considered the position estimate of the whole yacht. At the initial time $k = 1$, the position vector of the yacht is $\mathbf{x} = [0, 0]'$, and the yacht moves with a constant velocity of 10 m/s in the east and 20 m/s in north directions throughout the simulation. The simulation time is the 50 s, and the sampling time is 1 s. However, four GNSS receivers

TABLE 1. The initial values of right ascension and angular phase of the satellites.

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

TABLE 2. The relative position vector from the center of the yacht.

	receiver-1	receiver-2	receiver-3	receiver-4	spoofer
δ_x	-20	-15	45	35	0
δ_y	20	-30	-10	50	300

are deployed at different locations rather than installing the GNSS receiver at the center of the yacht. The RPV of the GNSS receivers concerning the vehicle center is tabulated in Table 2. The spoofer location from the center of the yacht is also presented in Table 2, and is shown in Fig. 3. We consider a false trajectory walking test bench [20] to evaluate the proposed algorithm. That is, consistently, the receiver is misled by constant distance, and the trajectory follows the constant velocity (CV) model as shown in Fig. 3. The spoofing process is carried out using a repeater-based spoofer. As given in [33], it is always advisable to maintain a constant distance between the spoofer and GNSS receiver to avoid anti-spoofing algorithms like power thresholding [34]. Therefore, the spoofer is 300 m away from the vehicle's center and travels parallel to the yacht throughout the simulation scenario.

The yacht turbulence modeled as a process noise. The state propagation is given by

$$X_j(k+1) = F_j(k)X_j(k) + p_j(k) \tag{54}$$

The process noise components along the east and north follows the white Gaussian with standard deviations of 1m and 1m respectively. The state vector is $[x\ y\ \dot{x}\ \dot{y}]'$ and the state transition is given by

$$F_j = \begin{bmatrix} 1 & 0 & \delta t & 0 \\ 0 & 1 & 0 & \delta t \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{55}$$

The δt is the sampling time equal to 1 s. The GNSS receivers are synchronous for the given sampling time and report the updated state by processing the received pseudorange measurements. The spoofing process starts at discrete time index $k = 20$; the simulation scenario of GNSS receivers and spoofer is as shown in Fig. 4. The true pseudorange measurements are corrupted with WGN noise with mean zero and standard deviation of 3 m. Due to the ideal spoofer assumption, the repeater-based spoofer also processes with the same noise statistics [23], i.e., the spoofed pseudorange measurements are also corrupted with WGN noise with zero mean and standard deviation of 3 m.

B. GNSS TRACKS ACCURACY

The position estimate of each GNSS receiver is obtained by using pseudorange measurements in the EKF framework.

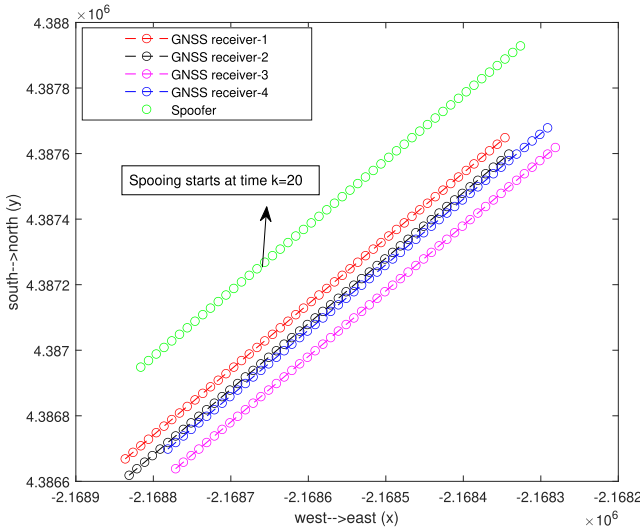

FIGURE 4. Positions of multiple GNSS receivers installed on a vehicle (ship) and spoofer.

The tunable parameters of the filter are its process noise covariance Q and measurement noise covariance R. All the GNSS receivers are given with

$$Q = q_\sigma \begin{bmatrix} \frac{\delta t^3}{3} & 0 & & 0 \\ 0 & \frac{\delta t^3}{3} & 0 & \frac{\delta t^2}{2} \\ \frac{\delta t^2}{2} & 0 & \delta t & 0 \\ 0 & \frac{\delta t^2}{2} & 0 & \delta t \end{bmatrix}, \quad R = \text{diag}(3^2, \cdots, 3^2). \tag{56}$$

Two point initialization method [32] is adopted to initialize the GNSS tracks at $k = 1$. The two point initialization uses the position estimates provided at $t(0)$ and $t(1)$ as

$$X(1) = \left[\mathbf{x}(1), \frac{\mathbf{x}(1) - \mathbf{x}(0)}{\delta t}\right]'. \tag{57}$$

Till $k = 20$, the GNSS receivers estimate the PVT correctly due to the reception of authentic measurements. At $k = 20$, spurious signals are locking onto the receiver, and the GNSS receiver estimates a false position owing to false pseudo-ranges. So in the absence of anti-spoofing algorithms, the position root mean square error (PRMSE) increases during the attack. Even though the spoofer intended to spoof the GNSS-1, all the four GNSS receivers are spoofed to different locations. Here, all the four GNSS receivers are involved in spoofing attacks due to the Omni-directional behavior of the spoofer [21]. Hence, in the spoofing activity, the PRMSE of the GNSS receivers is different under spoofer-to-receiver distance as given in (9). Therefore, throughout the spoofing attack, the PRMSE raises in the absence of anti-spoofing algorithms. The EKF estimation accuracy for all the GNSS receivers are depicted in Fig. 5a–Fig. 5d with four spoofed measurements.

In Fig. 5a, we can see that the spoofing attack leads to a rise in PRMSE to 16 m since the spoofer is intended to spoof GNSS-1 by 10 m along east and north. This implication of position spoofing does not imply equality on all the GNSS receivers. Because the spatial distance of GNSS receivers is different, hence we can observe that the GNSS-2, GNSS-3, GNSS-4 receivers are getting spoofed to different locations, and PRMSE is 40 m, 100 m, 100 m, respectively. In the initial phase of spoofing attack, i.e., at $k \in [21 - 23]$, the PRMSE rises because the filter gives more weight to measurement rather than prediction. In this process, the gain changes and tunes to the spoofed measurements. The sudden deflection in the measurement is considered as the outliers, and the filter cannot mitigate such outliers. The filter estimates the updated state based on the prediction and the available measurement at that time instant. In this process, the filter took four samples to reach the worst spoofing case (max value of spoofing deflection). We adopted the $1/3$ rule to make pseudo track updation and the $4/7$ rule to mitigate the effect. Therefore, as given in (46), the pseudo track is considered for the GNSS during the period of $k \in [21 - 24]$. After four data samples, i.e., at $k = 25$, the signals coming from the spoofers direction are not considered. Once this mitigation is performed, the actual measurements are getting locked onto the receivers. Therefore, the actual measurements are considered from $k = 25$ to perform the position estimate.

In the Fig. 5a–Fig. 5d, it is worth noting that the PRMSE raises during the interval of $k \in [21 - 24]$. This is due to the predicted state rather than the updated state. Hence, if a filter runs with the prediction, it cannot accommodate the turbulence, and an error is observed. The rise in PRMSE during this interval is around $2 - 4$ m. Since the vehicle is moving with the CV model, this error is less, and else we can see more error for turn and acceleration models. Therefore, this pseudo track updation is a suitable candidate for navigation in an intentional interference case for a lesser duration. Once the attack is detected, the vehicle can rely on the prediction of the track or inertial measurement units. Soon after the attack is mitigated, the filter again acquires the authentic measurements and computes the GNSS state. After mitigation, the filter again tunes to these measurements, and PRMSE decreases. This can be seen in the results that the PRMSE comes down from $k = 24$ and again settles.

C. VEHICLE POSITIONING

The vehicle positioning is the resultant of constructed equivalent measurements. Here, the equivalent measurements are translated and processed in batch LS framework to get the vehicle position. The vehicle position PRMSE is depicted in Fig. 6 with four GNSS receivers, and each receiver gets four pseudoranges. Here, we observe that in the spoofing case, the PRMSE increases, and the proposed method can maintain the track continuity with the help of a pseudo-track update. In the absence of anti-spoofing, the PRMSE vale is around $15 - 20$ m. Whereas, with the proposed method, the vehicle maintains the PRMSE value in the range of $2 - 4$m,

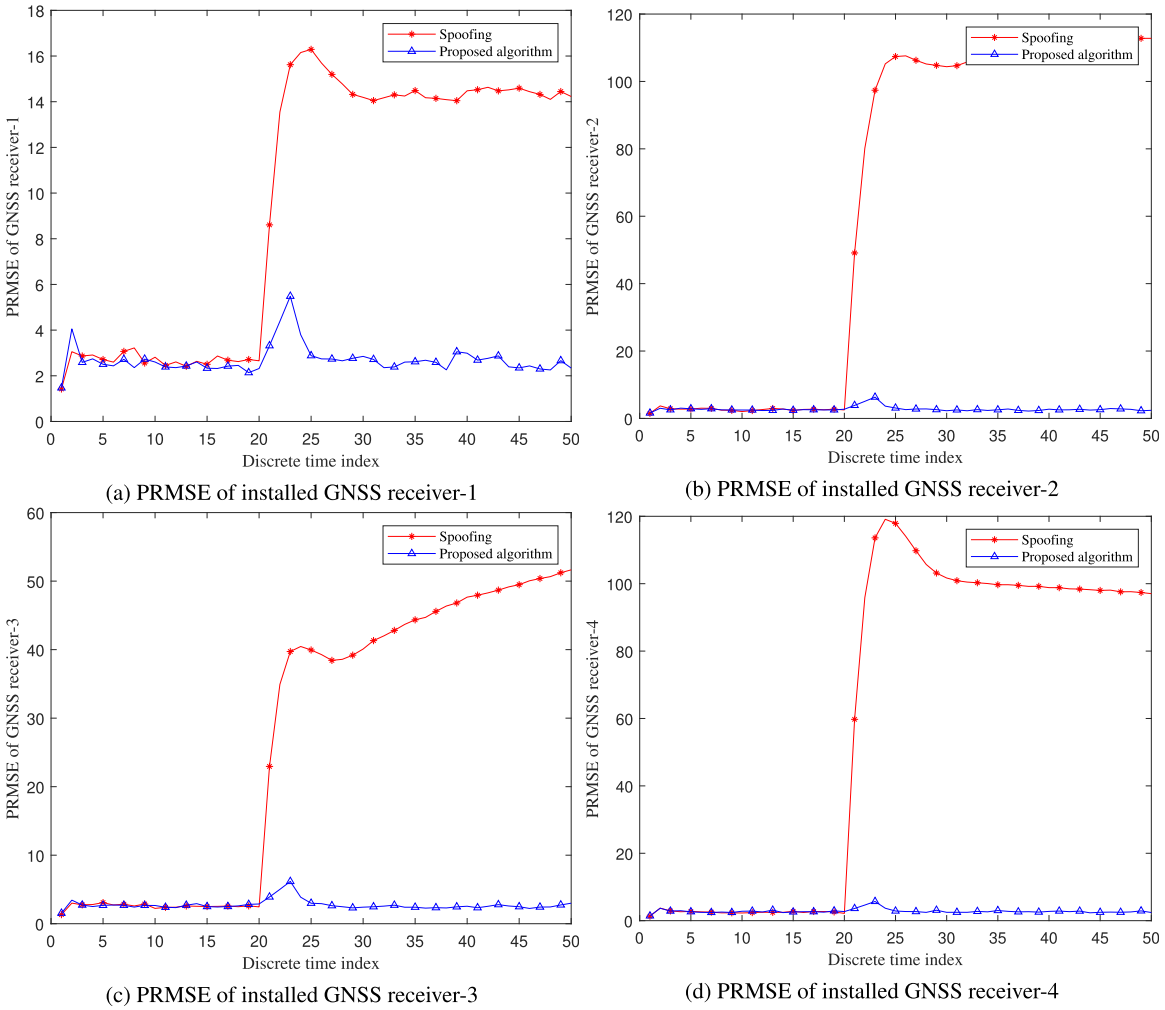

FIGURE 5. PRMSE of installed GNSS receivers with traditional and proposed algorithm in spoofing environment by using four satelite measurements.

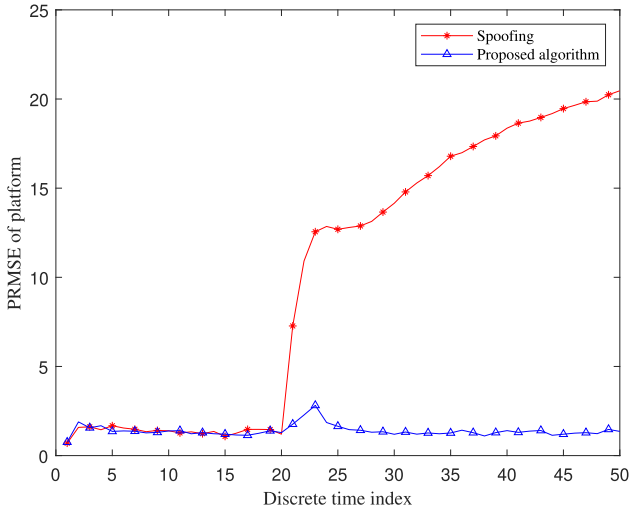

FIGURE 6. PRMSE of the vehicle by fusing all the pseudo-positions obtained by tracklet framework (four satellites are in range to GNSS receivers).

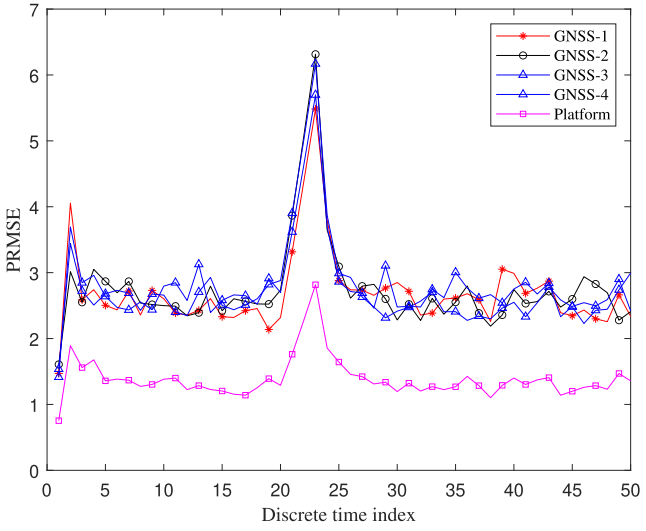

FIGURE 7. PRMSE of the vehicle by batch LS on equivalent measurements.

agreeing with the civilian GNSS receiver estimate. Moreover, this batch LS gives an enhanced estimate, and it is evident from Fig. 7. The individual GNSS receivers offer the PRMSE around 2.5 – 6 m, whereas the vehicle offers 1.5 – 3 m accuracy, almost two-fold improvement. This proposed method can work for spoofing detection and is a suitable candidate

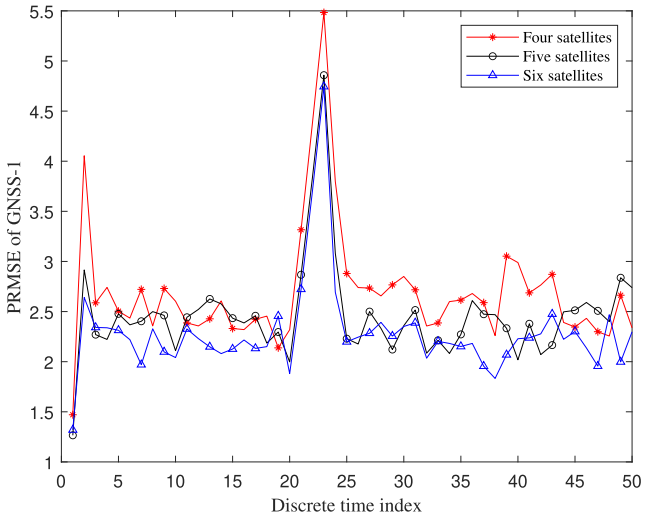

FIGURE 8. Comparison of PRMSE of GNSS-1 for various number of satellite signals.

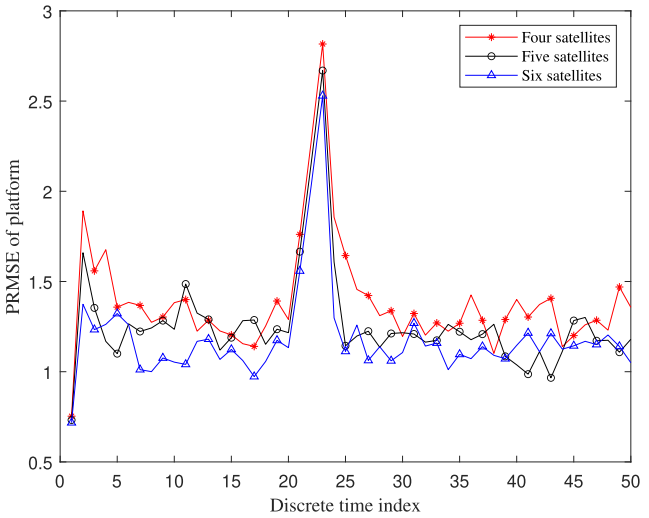

FIGURE 9. Comparison of PRMSE of vehicle for various number of satellite signals.

to process the multiple GNSS receiver's data to obtain the overall estimate of the vehicle.

D. IMPACT OF NUMBER OF SATELLITES

The number of available satellites is an essential parameter in pseudorange to position estimation. Here, the state of the GNSS consists of three parameters of interest. Hence, to estimate a position in 2D, one needs at least three pseudorange measurements. In this simulation, we varied the number of satellites from four to six. By varying the number of satellites, the PRMSE of the GNSS receiver-1 is depicted in Fig. 8, where we can see that the increase in satellite number increases the position estimate. The other GNSS receivers (GNSS receiver-2, 3, and 4) provide the same performance as shown in Fig. 8. Further, the vehicle PRMSE is also computed and visualized in Fig. 9. It is noticed that, as the satellite number increases, the vehicle position estimation accuracy improves.

E. ACCURACY OF LOCALIZATION AND MITIGATION

The localization of the spoofer helps to mitigate the spoofing attack. The localization of the spoofer is achieved by using bearings to position estimates in the ILS framework. Here, the bearings are corrupted with WGN with mean zero and standard deviation of 1 m rad. While performing the spoofer localization, the initial estimate of the spoofer's location is an intersection of two bearings. After that, we performed the ILS with the obtained bearings information. The number of iterations is limited based on the required accuracy over the time frames and is limited to 3 m. In another case, the maximum number of iterations is 20. Even though the position information of the GNSS receivers is calculated using the pseudo-update, we accomplished a good performance. The PRMSE of the spoofer is depicted in Fig 10.

The decision of spoofer mitigation is carried out by observing the spoofing attack detection over time. The m/n rule is adapted to make a decision. Here, for larger m, the vehicle

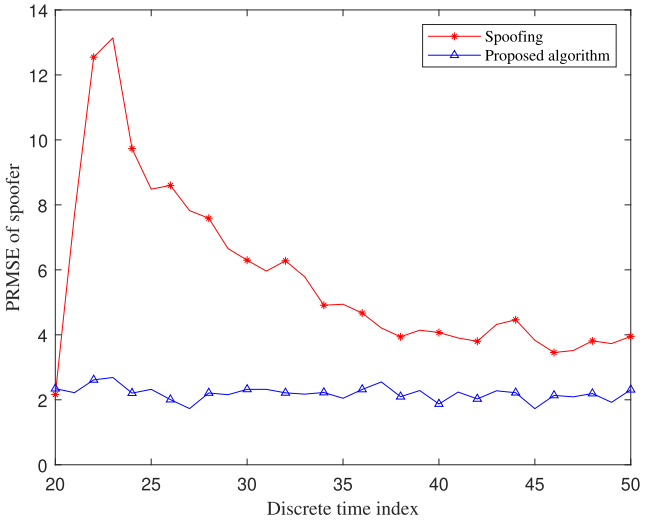

FIGURE 10. PRMSE of the spoofer (four satellites are in range to GNSS receivers).

tracking performance can be improved, but in the same duration, the GNSS track may attain higher PRMSE due to pseudo track update. Hence, to demonstrate the effect of the decision on several scans, we carried out the simulations for $m = 4$, 6, and 8. The PRMSE corresponding to GNSS-1 for the variable number of scans is presented in Fig. 11. This analogy is equally adapted for all the other GNSS receivers. We can observe a rise in PRMSE after $k = 20$ and before applying the mitigation. The PRMSE only increases because of the predicted state rather than the updated state during the duration of spoofing mitigation. Here, it is essential to note that this algorithm provides lower performance while mitigating the spoofing effect for a higher value of scan number. In Fig. 11, as the number of scans increases, the PRMSE increases. In addition, the same impact of scans has also been observed in vehicle positioning. In Fig. 12, the vehicle position accuracy can be observed, and it is also in

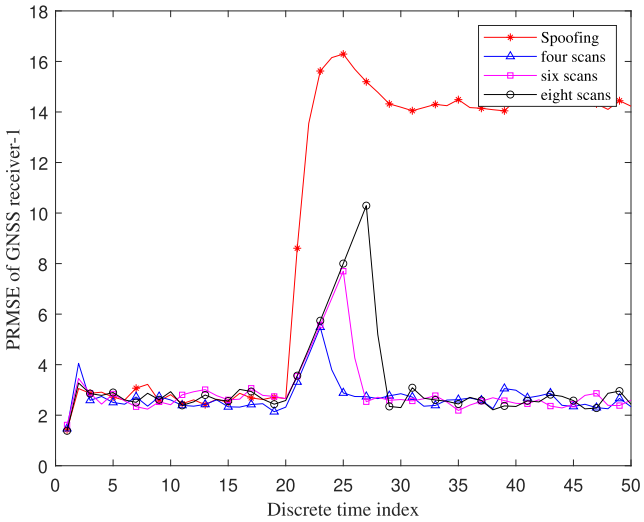

FIGURE 11. PRMSE of GNSS receiver −1 for variable number of decision on mitigation (four satellites are in range to GNSS receivers).

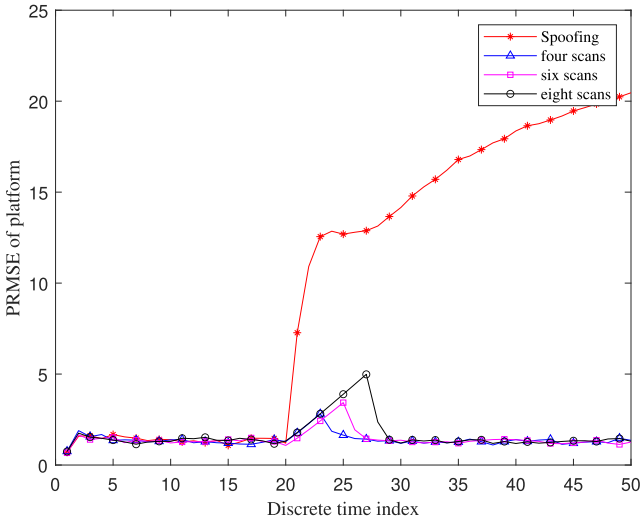

FIGURE 12. PRMSE of vehicle for variable number of decision on mitigation (four satellites are in range to GNSS receivers).

agreement with the GNSS receiver's accuracy. This rise in the PRMSE is owing to the batch estimate of the installed GNSS receivers. Even though the PRMSE increases, it is lower than the accuracy of installed GNSS receivers. Hence, this algorithm is equally deployable for larger scans to decide to spoof mitigation.

Furthermore, it is worth mentioning that this algorithm works for any number of GNSS receivers. As the number of installed GNSS receivers increases, the position estimate of the vehicle increases. This algorithm is evaluated on a vehicle, but this can be equally applied in the given surveillance, and it is easy to know the RPV while installing.

VI. CONCLUSION

This paper proposes the installation of multiple GNSS receivers on a vehicle to detect the spurious attacks and secure navigation. It assumes that the installed GNSS receiver's relative position vector (RPV) from the vehicle's center is known precisely. The generalized mathematical framework is derived for the multiple GNSS receivers in a spoofing environment. The pseudorange measurements of either authentic satellites or the spoofer are considered to estimate the receiver's state using the extended Kalman filter (EKF) framework. Once the states are available, an equivalent measurement in the cartesian domain is derived with the help of tracklets, and these tracklets are then translated using RPV. Besides, the vehicle location is calculated using the translated equivalent measurements in the batch least square (LS) framework. This paper considered two different spoofing attack detection tests: bearings-based detection and tracklets based detection. A generalized likelihood ratio test is developed using the translated equivalent measurements to distinguish the spoofing and non-spoofing cases. Soon after the threat is detected, an iterative least square (ILS) based localization framework is employed to localize the spoofer, using the bearings-only information. However, the estimated GNSS location is falsified due to the spoofed location at that specific epoch. Hence, this paper employed a pseudo track update to calculate the receiver's position at that epoch. The simulation results reveal that installing a number of GNSS receivers not only detects the spoofing attack but also enhances the vehicle position estimate. Further, it is observed from the results that, as the number of satellite signals increases, the proposed algorithm provides improved PRMSE for all GNSS receivers, location accuracy of vehicle, and spoofer location.

This paper can be further extended to the specific surveillance area, as RPV calculation for a static node is feasible. This tracklet based equivalent measurement re-creation approach is a generalized technique, which is sensor measurement independent and can be applied for all other sensors. Furthermore, we limited this work to the static installation of the node; however, one can look into the problem of dynamic nodes and develop novel algorithms as future work.

APPENDIX

The section provides the detailed derivation of the equivalent measurement covariance in (25).

By using the properties

$$\mathbb{E}\left[\tilde{m}_j(k,k') \mid \mathbf{Z}_j^{k'}\right] = 0. \tag{58}$$

$$\mathbb{E}\left[\tilde{m}_j(k,k') \mid \mathbf{Z}_j^{k}\right] \neq 0. \tag{59}$$

and

$$\begin{aligned}
&\mathbb{E}\left[\hat{X}_j(k|k)\hat{X}_j(k|k') \mid \mathbf{Z}_j^{k'}\right] \\
&= \mathbb{E}[\mathbb{E}[[X_j(k) - \hat{X}_j(k|k)] \\
&\quad \times [X_j(k) - \hat{X}_j(k|k) + \hat{X}_j(k|k) - \hat{X}_j(k|k')]^T \mid \mathbf{Z}_j^{k}] \mid \mathbf{Z}_j^{k'}] \\
&= \mathbb{E}\left[\mathbb{E}\left[[X_j(k) - \hat{X}_j(k|k)][X_j(k) - \hat{X}_j(k|k)]^T \mid \mathbf{Z}_j^{k}\right] \mid \mathbf{Z}_j^{k'}\right] \\
&\quad + \mathbb{E}\left[\mathbb{E}\left[[X_j(k) - \hat{X}_j(k|k)] \mid \mathbf{Z}_j^{k}\right]\right. \\
&\quad \times \left.\left[\hat{X}_j(k \mid k) - \hat{X}_j(k|k')\right]^T\right] \mid \mathbf{Z}_j^{k'}\Big]
\end{aligned}$$

$$= \mathbf{P}_j(k \mid k) \tag{60}$$

In the above, it is to be noted that, the term $\mathbb{E}\left[[X_j(k) - \hat{X}_j(k|k)] \mid \mathbf{Z}_j^k\right]$ is zero. The $M_j(k, k')$ can be expanded as

$$\begin{aligned} M_j(k,k') &= \mathbb{E}\left[\tilde{m}_j(k,k')\tilde{m}_j(k,k')^T \mid \mathbf{Z}_j^{k'}\right] \\ &= A_j(k|k')\mathbf{P}_j(k \mid k)A_j(k|k')^T \\ &\quad + \left[A_j(k|k') - \mathbf{I}\right]\mathbf{P}_j(k \mid k')\left[A_j(k|k') - \mathbf{I}\right]^T \\ &\quad - A_j(k|k')\mathbf{P}_j(k \mid k)\left[A_j(k|k') - \mathbf{I}\right]^T \\ &\quad - \left[A_j(k|k') - \mathbf{I}\right]\mathbf{P}_j(k \mid k)A_j(k|k') \\ &= \left[A_j(k|k') - \mathbf{I}\right]\mathbf{P}_j(k \mid k')\left[A_j(k|k') - \mathbf{I}\right]^T \\ &\quad - A_j(k|k')\mathbf{P}_j(k \mid k)A_j(k|k')^T + A_j(k|k')\mathbf{P}_j(k \mid k) \\ &\quad + \mathbf{P}_j(k \mid k)A_j(k|k')^T \end{aligned} \tag{61}$$

Now, by using the property

$$\begin{aligned} &\left[A_j(k|k') - \mathbf{I}\right]\mathbf{P}_j(k \mid k') \\ &= \left[\mathbf{P}_j(k \mid k')\left[\mathbf{P}_j(k \mid k') - \mathbf{P}_j(k \mid k)\right]^{-1} - \mathbf{I}\right]\mathbf{P}_j(k \mid k') \\ &= \mathbf{P}_j(k \mid k')\left[\left[\mathbf{P}_j(k \mid k') - \mathbf{P}_j(k \mid k)\right]^{-1} - \mathbf{P}_j(k \mid k')^{-1}\right] \\ &\quad \times \mathbf{P}_j(k \mid k') \\ &= \mathbf{P}_j(k \mid k')\left[\mathbf{P}_j(k \mid k') - \mathbf{P}_j(k \mid k)\right]^{-1} \\ &\quad \times \left[\mathbf{I} - [\mathbf{P}_j(k \mid k') - \mathbf{P}_j(k \mid k)]\mathbf{P}_j(k \mid k)^{-1}\right]\mathbf{P}_j(k \mid k') \\ &= A_j(k|k')\left[\mathbf{I} - \mathbf{I} + \mathbf{P}_j(k \mid k)\mathbf{P}_j(k \mid k')^{-1}\right]\mathbf{P}_j(k \mid k') \\ &= A_j(k|k')\mathbf{P}_j(k \mid k) \end{aligned} \tag{62}$$

Therefore, the $M_j(k, k')$ can be further simplified as

$$\begin{aligned} M_j(k,k') &= \left[A_j(k|k')\right]\mathbf{P}_j(k \mid k')\left[A_j(k|k') - \mathbf{I}\right]^T \\ &\quad - A_j(k|k')\mathbf{P}_j(k \mid k)A_j(k|k')^T + A_j(k|k')\mathbf{P}_j(k \mid k) \\ &\quad + \mathbf{P}_j(k \mid k)A_j(k|k')^T \\ &= \left[A_j(k|k')\right]\mathbf{P}_j(k \mid k')A_j(k|k')^T - A_j(k|k')\mathbf{P}_j(k \mid k) \\ &\quad - A_j(k|k')\mathbf{P}_j(k \mid k)A_j(k|k')^T + A_j(k|k')\mathbf{P}_j(k \mid k) \\ &\quad + \mathbf{P}_j(k \mid k)A_j(k|k')^T \\ &= \mathbf{P}_j(k \mid k)A_j(k|k')^T \end{aligned} \tag{63}$$

which yields (25). It is important to note that (62) and (63) are transpose of each other. However, since $M_j(k, k')$ is symmetric, (62) and (63) are equal to each other.

ACKNOWLEDGMENT

The first and second authors would like to thank Prof. T. Kirubarajan and Dr. R. Tharmarasa for providing valuable inputs during the stay in ETF Laboratory, McMaster University, Canada as a visiting students during 2018-19.

REFERENCES

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

[2] Q. Meng, L.-T. Hsu, B. Xu, X. Luo, and A. El-Mowafy, "A GPS spoofing generator using an open sourced vector tracking-based receiver," *Sensors*, vol. 19, no. 18, p. 3993, Sep. 2019.

[3] J. Warner and R. Johnston, "A simple demonstration that the global positioning system (GPS) is vulnerable to spoofing," *J. Secur. Admin.*, vol. 25, no. 2, pp. 19–28, 2002.

[4] 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.

[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, pp. 64:1–64:31, May 2016.

[6] 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.

[7] M. Appel, A. Konovaltsev, and M. Meurer, "Robust spoofing detection and mitigation based on direction of arrival estimation," in *Proc. 28th Int. Tech. Meeting Satell. Division Inst. Navigat. (ION GNSS)*, 2015, pp. 3335–3344.

[8] E. Axell, E. G. Larsson, and D. Persson, "GNSS spoofing detection using multiple mobile COTS receivers," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Apr. 2015, pp. 3192–3196.

[9] Z. Zhang and X. Zhan, "GNSS spoofing network monitoring based on differential pseudorange," *Sensors*, vol. 16, no. 10, p. 1771, Oct. 2016.

[10] F. Wang, H. Li, and M. Lu, "GNSS spoofing detection based on unsynchronized double-antenna measurements," *IEEE Access*, vol. 6, pp. 31203–31212, 2018.

[11] B. Pardhasaradhi, P. Srihari, and P. Aparna, "Spoofer-to-target association in multi-spoofer multi-target scenario for stealthy GPS spoofing," *IEEE Access*, vol. 9, pp. 108675–108688, 2021.

[12] P. F. Swaszek, R. J. Hartnett, and K. C. Seals, "Using range information to detect spoofing in platoons of vehicles," in *Proc. 30th Int. Tech. Meeting Satell. Division Inst. Navigat. (ION GNSS)*, 2017, pp. 2838–2853.

[13] J. A. Bhatti, T. E. Humphreys, and B. M. Ledvina, "Development and demonstration of a TDOA-based GNSS interference signal localization system," in *Proc. IEEE/ION PLANS*, Apr. 2012, pp. 455–469.

[14] A. Perkins, L. Dressel, S. Lo, and P. Enge, "Antenna characterization for UAV based GPS jammer localization," in *Proc. 28th Int. Tech. Meeting Satell. Division Inst. Navigat. (ION GNSS)*, 2015, pp. 1684–1695.

[15] D. Fontanella, R. Bauernfeind, and B. Eissfeller, "In car GNSS jammer localization using vehicular ad-hoc network," *Inside GNSS*, vol. 11, pp. 70–80, 2013.

[16] S. Bhamidipati and G. X. Gao, "Locating multiple GPS jammers using networked UAVs," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1816–1828, Apr. 2019.

[17] S. Shang, H. Li, C. Peng, and M. Lu, "A novel method for GNSS meaconer localization based on a space–time double-difference model," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 56, no. 5, pp. 3432–3449, Oct. 2020.

[18] K. Jansen, M. Schäfer, V. Lenders, C. Pöpper, and J. Schmitt, "Localization of spoofing devices using a large-scale air traffic surveillance system," in *Proc. ACM Asia Conf. Comput. Commun. Secur.*, 2017, pp. 914–916.

[19] C. Sanders and Y. Wang, "Localizing spoofing attacks on vehicular GPS using Vehicle-to-Vehicle communications," *IEEE Trans. Veh. Technol.*, vol. 69, no. 12, pp. 15656–15667, Dec. 2020.

[20] P. Bethi, S. Pathipati, and A. P, "Stealthy GPS spoofing: Spoofer systems, spoofing techniques and strategies," in *Proc. IEEE 17th India Council Int. Conf. (INDICON)*, Dec. 2020, pp. 1–7.

[21] 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.

[22] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "Unmanned aircraft capture and control via GPS spoofing," *J. Field Robot.*, vol. 31, no. 4, pp. 617–636, 2014.

[23] P. Bethi, S. Pathipati, and A. P, "Impact of target tracking module in GPS spoofer design for stealthy GPS spoofing," in *Proc. IEEE 17th India Council Int. Conf. (INDICON)*, Dec. 2020, pp. 1–6.

[24] O. E. Drummond, "Hybrid sensor fusion algorithm architecture and tracklets," in *Signal Data Process. Small Targets 1997*, vol. 3163. SPIE, 1997, pp. 485–502.

[25] O. E. Drummond, "Track and tracklet fusion filtering," in *Signal and Data Processing of Small Targets*, vol. 4728. Orlando, FL, USA, International Society for Optics and Photonics, 2002, pp. 176–195.

[26] D. Huang, H. Leung, and E. Bosse, "A pseudo-measurement approach to simultaneous registration and track fusion," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 48, no. 3, pp. 2315–2331, Jul. 2012.
[27] Y. Bar-Shalom, X. R. Li, and T. Kirubarajan, *Estimation With Applications to Tracking and Navigation: Theory Algorithms and Software*. Hoboken, NJ, USA: Wiley, 2004.
[28] S. M. Kay, *Fundamentals of Statistical Signal Processing: Estimation Theory*, vol. I. Englewood Cliffs, NJ: Prentice-Hall 1993.
[29] P. Bethi, S. Pathipati, and A. P, "GNSS intentional interference mitigation via average KF innovation and pseudo track updation," in *Proc. IEEE 17th India Council Int. Conf. (INDICON)* New Delhi, India, Dec. 2020, pp. 1–5.
[30] H. C. So, "Source localization: Algorithms and analysis," in *Handbook of Position Location: Theory, Practice, and Advances*. 2011, pp. 25–66.
[31] S. Daneshmand, A. Jafarnia-Jahromi, A. Broumandon, and G. Lachapelle, "A low-complexity GPS anti-spoofing method using a multi-antenna array," in *Proc. 25th Int. Tech. meeting Satell. Division Inst. Navigat. (ION GNSS)*, 2012, pp. 1233–1243.
[32] Y. Bar-Shalom, P. K. Willett, and X. Tian, *Tracking and Data Fusion*, vol. 11. Storrs, CT, USA: YBS publishing Storrs, 2011.
[33] J. S. Warner and R. G. Johnston, "A simple demonstration that the global positioning system (GPS) is vulnerable to spoofing," *J. Secur. Admin.*, vol. 25, no. 2, pp. 19–27, 2002.
[34] 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.

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

GUNNERY SRINATH (Graduate Student Member, IEEE) received the B.Tech. degree in electronics and communication engineering from Jawaharlal Nehru Technological University, Anantapur, India, in 2013, and the M.Tech. degree in digital communication from ABV-IIITM, Gwalior, India, in 2016. He is currently pursuing the Ph.D. degree in electronics and communication engineering with the National Institute of Technology Karnataka, Surathkal, Mangaluru, India. From 2018 to 2019, he was a Visiting Ph.D. Student with the Estimation, Tracking and Fusion Research Laboratory, McMaster University, Hamilton, Ontario, Canada. His research interests include cognitive radio, radar signal processing, radar and communication system spectrum sharing, and target tracking.

G. S. VANDANA (Member, IEEE) received the B.Tech. degree in electronics and communication engineering from Vishveshvaraya Technological University, Karnataka, India, in 2014, and the M.Tech. degree in digital electronics and communication from the N. M. A. M. Institute of Technology, Karnataka, India, in 2016. She is currently working as a Project Development Manager with Sri Shasha Prayathi Technologies Private Ltd. Her research interests include real time applications on radar sensor, radar signal processing, and target tracking.

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 the field of 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 a Senior Member of ACM. He is a fellow of IETE and a member of IEICE, Japan. He received 2010 IEEE Asia Pacific Outstanding Branch Counselor Award. He received the 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, where she has been working as an Assistant Professor, since 2008. She has conducted a number of workshops in the area of embedded systems and ARM processor. She has published more than 25 research papers in various journals and conference proceedings. She has guided two Ph.D. student and currently guiding five other research students. She is currently 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. Her research interests include bio-medical signal processing, signal compression, computer architecture, and embedded systems. She has presented a number of research papers in various international conferences.