Kalantari and Larsson *EURASIP Journal on Advances in Signal Processing* (2020) 2020:8
https://doi.org/10.1186/s13634-020-0663-z

EURASIP Journal on Advances in Signal Processing

RESEARCH Open Access

Statistical test for GNSS spoofing attack detection by using multiple receivers on a rigid body

Ashkan Kalantari[1] and Erik G. Larsson[2*]

Abstract

Global navigation satellite systems (GNSS) are being the target of various jamming, spoofing, and meaconing attacks. This paper proposes a new statistical test for the presence of multiple spoofers based on range measurements observed by a plurality of receivers located on a rigid body platform. The relative positions of the receivers are known, but the location and orientation of the platform are unknown. The test is based on the generalized likelihood ratio test (GLRT) paradigm and essentially performs a consistency check between the set of observed range measurements and known information about the satellite topology and the geometry of the receiver constellation. Optimal spoofing locations and optimal artificial time delays (as induced by the spoofers) are also determined.

Exact evaluation of the GLRT requires the maximum-likelihood estimates of all parameters, which proves difficult. Instead, approximations based on iterative algorithms and the squared-range least squares algorithm are derived. The accuracy of these approximations is benchmarked against Cramér-Rao lower bounds.

Numerical examples demonstrate the effectiveness of the proposed algorithm and show that increasing the number of GNSS receivers makes the attack easier to detect. We also show that using multiple GNSS receivers limits the availability of optimal attack positions.

Keywords: Global navigation satellite systems (GNSS), Spoofing, Generalized likelihood ratio test (GLRT)

1 Introduction

Global navigation satellite system (GNSS) technology provides real-time positioning for various civil and military applications. Due to the low received power (about −160 dBW), GNSS is highly susceptible to intentional and unintentional interference. In addition, the signal and modulation formats of civilian GNSS are publicly available. For these reasons, a wide range of attacks on GNSS are viable.

Attacks on GNSS are categorized into jamming, meaconing (replay), and spoofing [1]. In a *jamming* attack, the adversary overshadows the received GNSS signals with a higher power noise-like signal to make the receiver unable to decode the signal. In *meaconing* (replay), the adversary records the original GNSS signal and broadcasts it with a delay. In a *spoofing* attack, the attacker produces counterfeit GNSS signals that are similar to authentic ones, by modifying the original GNSS signals [2] in order to manipulate the victim receiver's estimated position. This attack might be the most hazardous since it can take place without the victim being aware of being attacked. In the most sophisticated spoofing attacks, the adversary uses multiple, coordinated spoofers. Owing to the availability of inexpensive software-defined radios and GNSS modules, it has become relatively easy to implement such attacks. This paper is concerned with sophisticated spoofing attacks.

1.1 Taxonomy of existing GNSS spoofing mitigation methods

There has been research in the past on defense mechanisms against GNSS spoofing attacks. Here, we categorize these techniques into three groups.

*Correspondence: erik.g.larsson@liu.se
Ashkan Kalantari produced this work while working as a Postdoctoral researcher in the Department of Electrical and Computer Engineering (ISY), Linköping University, Sweden.
[2]Department of Electrical and Computer Engineering (ISY), Linköping University, 581 83 Linköping, Sweden
Full list of author information is available at the end of the article

1.1.1 Techniques using auto-correlation characteristics

The first group of techniques uses the received signal auto-correlation function characteristics to detect the presence of a spoofer. These methods detect the spoofer when it tries to take over the tracking loop of the GNSS receiver. There are in turn three main approaches:

- Methods that use the signal quality monitoring mechanism to measure the distortion in the auto-correlation function of the received signal and detect the spoofer [3–12]. The paper [12] studies the applicability of multi-path mitigation techniques for anti-spoofing purposes. A different approach is taken in [13], where the cross-correlation among the GNSS signal of multiple GNSS receivers is used as input to a machine-learning classifier (a support vector machine specifically) to detect the spoofing attack.
- Considering that the spoofer must use higher power than the original GNSS signals to make the receiver lock on the counterfeit signals, monitoring the received power level of the auto-correlation function can be used to detect the spoofing attack [14–19]. The dynamic process of taking over the victim tracking loop is used in [19] to detect a spoofing attack. As a new metric, [18] proposes to measure the variance of the signal quality to detect when the spoofer starts taking over the tracking loop of the victim.
- One may combine both power and distortion monitoring of the auto-correlation function to detect an attack [20, 21].

These approaches have a number of difficulties. First, multi-path fading can cause distortion and power level fluctuations in the auto-correlation function of the received GNSS signal similar to those caused by the spoofer. In addition, the spoofer can intelligently change its power level to mimic the power fluctuation of multi-path fading. Second, these techniques require access to the received raw GNSS signals.

1.1.2 Spatial signal processing techniques

The second group of methods use spatial signal processing techniques to detect the presence of spoofers. These techniques can be further subdivided as:

- Spoofing detection maybe based on estimated direction-of-arrival of the GNSS signals [22–31]. Considering a common source of spoofing signals, the work [29] uses the time difference of arrival of the GNSS signal to detect spoofing. The work in [30] uses array processing along with multi-path detection algorithms to estimate the direction of arrival to detect the presence of one spoofer. A statistical test is used in [31] to estimate the power and angle-of-arrival of the GNSS signal in order to detect spoofing. For example, carrier phase differences can be used to estimate this direction of arrival [22, 25, 27].
- One may exploit that counterfeit signals from a single spoofing source are spatially correlated and measure the spatial correlation between the received signals from different satellites [32–34]. The work [34] uses correlation at multiple receivers to separately classify authentic and spoofing signals; then, double differences of carrier phase measurements are used to detect the spoofer.
- Using rotating antennas to measure the spatial correlation of the received GNSS signals [35, 36]. The paper [35] uses rotating antennas to measure the correlation between the carrier phases, while [36] uses a single rotating antenna to perform spatial power measurements.

The techniques in [22–28, 35, 36] require modification of the GNSS receiver hardware. In addition, the methods [22–28, 35, 36] are based on the property that the signals coming from a single-antenna spoofer are correlated. Attacks using multiple spoofers can result in spatially uncorrelated spoofing signals, in which case these methods can fail.

1.1.3 Methods that use multiple GNSS receivers

The last category of spoofing mitigation methods uses multiple GNSS receivers to detect the presence of the spoofer. These works can be further grouped as follows:

- Using multiple GNSS receivers to detect the presence of a spoofer, exploiting the fact that all GNSS receivers show the same position while being spoofed [37–42].
- Range measurements may be used directly to detect the spoofing attack [43–47]. More specifically, [43] considers multiple vehicles where each of them is equipped with a GNSS receiver and a range measurement sensor. The range measurements and GNSS positions are fused to detect the presence of one spoofer while assuming that only one of the vehicles is subject to a spoofing attack. In [44], the range measurements from multiple GNSS receivers are used to detect a spoofer, assuming that all range measurements from a spoofer are the same. Considering the effect of clock knowledge, the authors in [45] develop a technique to detect a spoofer using range measurements of multiple GNSS receivers. The authors of [46] propose to use the time difference of arrival of the GNSS signals derived from pseudorange measurements to detect the presence of one spoofer. The technique is based on the fact that signals coming from a spoofer have similar time differences of arrival. The work [47] studies detection of one spoofer using differential pseudorange and

carrier phase measurements by a double antenna receiver. The effect of synchronization between the measurements on spoofing detection is investigated.

All above methods except [41] consider the detection of a single-antenna spoofer. The paper [41] develops a technique for multi-antenna spoofer detection and presents implementation results.

1.2 Contributions

In this paper, we propose a signal processing approach that uses range measurements from multiple satellites to multiple GNSS receivers to detect the presence of multiple single-antenna spoofers. Each spoofer emulates one specific satellite. The GNSS receivers are assumed to be fixed on a rigid body platform (with known *relative* positions), and the range measurements gathered by all receivers are processed jointly to detect the presence of a spoofing attack. The technique developed here can work as a second layer of security to further strengthen methods that rely on properties of the auto-correlation function of the GNSS signal to detect spoofing attack (Section 1.1.1).

We make the following specific contributions:

- We cast the spoofing detection problem as a statistical hypothesis test, specifically a generalized likelihood ratio test (GLRT), based on a set of observed range measurements.
- We use squared range-least squares (SR-LS) approach [48] to approximately find maximum-likelihood estimates of the parameters under two hypotheses corresponding to spoofing and no spoofing, respectively. We also calculate the Cramér-Rao lower bound (CRLB) for the estimated parameters under both these hypotheses and compare the empirical results with these bounds.
- We determine optimal locations of the spoofers (from the adversary's perspective) that best counteract the proposed defense mechanism.

We present and evaluate all methodology using a two-dimensional model of the world, leaving the extension to three dimensions—which incurs some nontrivial technicalities—to future work.

1.3 Notation

Uppercase and lowercase bold-faced letters are used to denote matrices and column vectors, respectively. The superscripts $(\cdot)^T$, $(\cdot)^*$, $(\cdot)^H$, and $(\cdot)^\dagger$ denote the transpose, conjugate, Hermitian, and Moore-Penrose pseudo-inverse operators, respectively. $\mathbf{I}_{N\times N}$ denotes an N by N identity matrix, diag($\mathbf{a}$) denotes a diagonal whose diagonal elements are the elements of the vector $\mathbf{a}$, $\mathbf{0}$ is the all-zero vector, $\|\cdot\|$ is the Frobenius norm, and $|\cdot|$ represents the absolute value of a scalar. For a symmetric matrix $\mathbf{A}_{n\times n}$ and a positive definite matrix $\mathbf{B}_{n\times n}$, the generalized eigenvalues of the matrix pair $(\mathbf{A},\mathbf{B})$ are given by $\lambda_i(\mathbf{A},\mathbf{B}) = \lambda_i\left(\mathbf{B}^{-1/2}\mathbf{A}\mathbf{B}^{-1/2}\right)$, $i = 1,...,n$ where $\lambda_i(\mathbf{M})$ denotes the ith largest eigenvalue of $\mathbf{M}$.

Table 1 Summary of model parameters

Parameter	Description
M	Number of captured range measurements of a satellite or spoofer signal by a GNSS receiver
N	Number of GNSS receivers
I	Number of satellites
$\mathbf{p}_{n_0}$	Position of the nth GNSS receiver, relative to the platform
$\mathbf{s}_i$	Position of the ith satellite
$\mathbf{b}_0$	Translation vector of the platform
$\mathbf{T}$	Rotation matrix of the platform
$\mathbf{p}_i^A$	Position of the ith spoofer
τ_i	Artificial time delay induced by the ith spoofer
$r_{n,i,m}$	mth sample from the ith satellite or spoofer signal measured by the nth GNSS receiver
$n_{n,i,m}$	Noise component of $r_{n,i,m}$
σ^2	Noise power

2 System model and problem description

We consider a two-dimensional scenario with N GNSS receivers and I satellites. The GNSS receivers are mounted on a rigid platform with fixed (and known) mutual distances. We assume that the clocks of the GNSS receivers are synchronized with those of the satellites. Spoofers may be present, and if so, each spoofer emulates one specific satellite. The emulation is done by receiving the GNSS signal of a satellite, modifying the ephemeris data, adding an artificial time delay, and re-transmitting the signal [49]. We assume that the spoofers use higher transmit power than the satellites, so that the GNSS receivers lock on the spoofing signals instead of the legitimate satellite signals. When the receivers are synchronized, they can operate as a virtual array to perform angle-of-arrival estimation [50]. This can be used for spoofing detection where emulated GNSS signals arrive from a specific direction. In contrast, our approach can detect a spoofing attack where multiple spoofers emulate GNSS signals originating from geographically different locations. In addition, performing array processing requires accessing to the baseband signal of the GNSS receivers, which requires hardware modifications and precludes the use of commercial off-the-shelf (COTS) receivers.

Let $\mathbf{p}_n$ be the position of the nth GNSS receiver. Since the GNSS receivers are fixed on a rigid body, we can parameterize their positions in terms of their locations

relative to the platform, $\mathbf{p}_{n_0}$, a translation vector (that determines the position of the platform), $\mathbf{b}_0$, and a rotation matrix (that determines the orientation of the platform), $\mathbf{T}$, according to

$$\mathbf{p}_n = \mathbf{b}_0 + \mathbf{T}\mathbf{p}_{n_0}. \tag{1}$$

The rotation matrix, $\mathbf{T}$, is parameterized in terms of a rotation angle θ as

$$\mathbf{T} = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}, \tag{2}$$

and we write $\mathbf{b}_0 = \begin{bmatrix} b_{01} \\ b_{02} \end{bmatrix}$. Hence, $\{\mathbf{p}_{n_0}\}$ are known a priori, while $\mathbf{b}_0$ and $\mathbf{T}$ are not. Figure 1 illustrates the relation between the variables $\{\mathbf{p}_n\}$, $\mathbf{b}_0$, $\mathbf{T}$, and $\{\mathbf{p}_{n_0}\}$ in (1).

Each GNSS receiver takes M range measurements to each satellite. To detect the possible presence of spoofers, we apply a binary hypothesis test to the so-obtained range measurements. In regular operation (no spoofing), the delay of a signal from a satellite to a receiver is entirely due to the physical distance. In contrast, in the presence of spoofing, the spoofer is generally located at a different position than the satellite, and it can add an artificial, a priori unknown, time delay to the GNSS signal to simulate a different physical distance. Therefore, the two hypotheses, regular operation ($\mathcal{H}_0$) and spoofing ($\mathcal{H}_1$) cases, can be formulated:

$$\mathcal{H}_0 : r_{n,i,m} = \left\| \mathbf{b}_0 + \mathbf{T}\mathbf{p}_{n_0} - \mathbf{s}_i \right\| + n_{n,i,m}, \tag{3}$$

$$\mathcal{H}_1 : r_{n,i,m} = \left\| \mathbf{b}_0 + \mathbf{T}\mathbf{p}_{n_0} - \mathbf{s}_i^{'} \right\| + \tau_i + n_{n,i,m}. \tag{4}$$

where $1 \le n \le N$, $1 \le i \le I$, and $1 \le m \le M$ is the number of GNSS signal samples captured by each GNSS receiver. We assume that the rigid body does not move during the sampling. Here, $n_{n,i,m}$ are measurement noise samples that we model as identically distributed zero-mean Gaussian random variables with variance σ^2, and we assume that these noise samples are independent among n, i, and m. Also, $\mathbf{s}_i$ is the true position of the ith satellite, $\mathbf{s}_i^{'}$ is the forged position of the ith satellite (when a spoofer is present), and τ_i is the artificial time delay caused by the ith spoofer. Note that the artificial time delay introduced by the spoofer is perceived by the GNSS receivers as an additional propagation distance. We assume that the noise power, σ^2 is known by the GNSS receivers (Table 1).

Under $\mathcal{H}_1$, the translation vector $\mathbf{b}_0$ is the same for all measurements, and hence we can absorb $\mathbf{b}_0$ into the unknown satellite positions $\mathbf{s}_i^{'}$ by rewriting (4) as

$$\mathcal{H}_1 : r_{n,i,m} = \left\| \mathbf{T}\mathbf{p}_{n_0} + \mathbf{s}_i^{''} \right\| + \tau_i + n_{n,i,m}, \tag{5}$$

where

$$\mathbf{s}_i^{''} = \mathbf{b}_0 - \mathbf{s}_i^{'}.$$

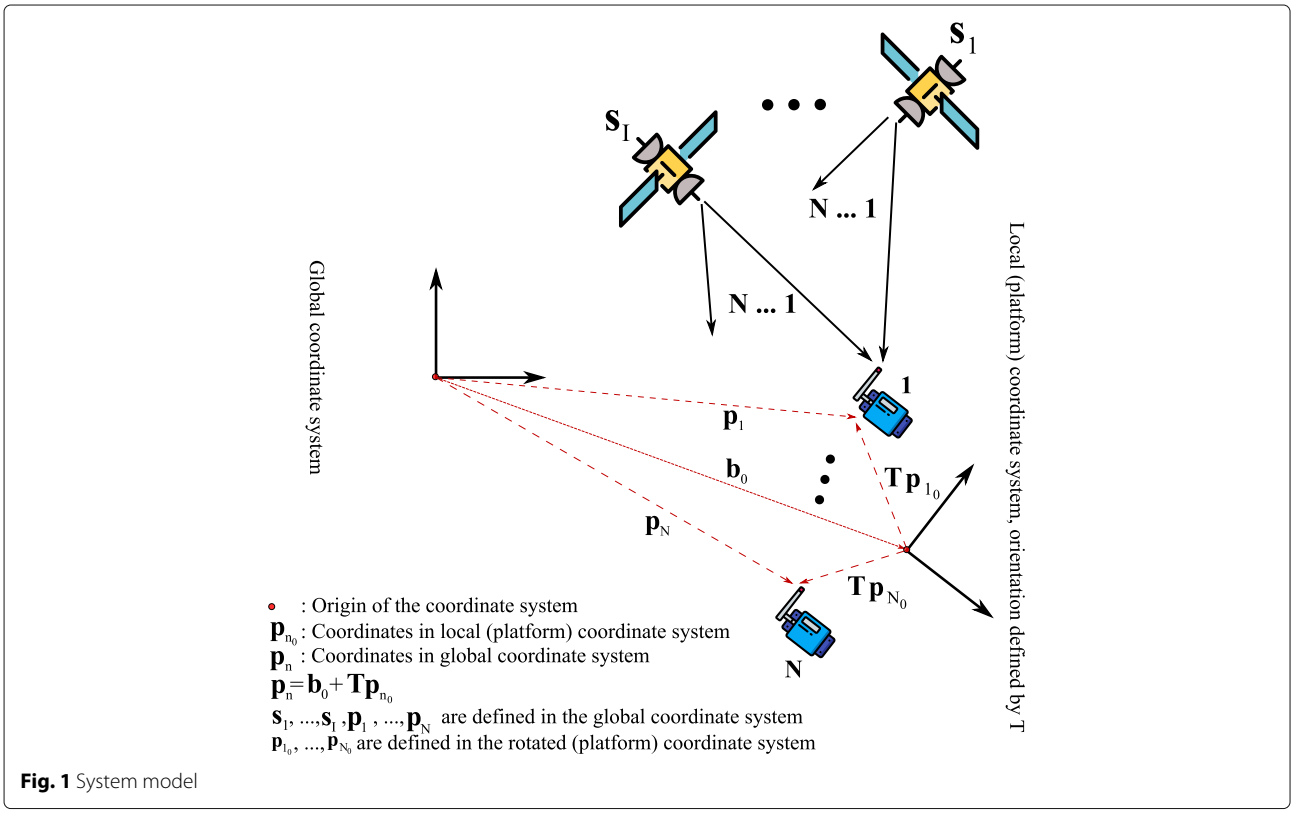

Fig. 1 System model

To further simplify (5), we can factor out the rotation matrix $\mathbf{T}$, exploiting that $\mathbf{T}^T\mathbf{T} = \mathbf{I}$, to rewrite (5) as

$$\mathcal{H}_1 : r_{n,i,m} = \left\| \mathbf{p}_{n_0} + \mathbf{s}_i''' \right\| + \tau_i + n_{n,i,m}, \tag{6}$$

where

$$\mathbf{s}_i''' = \mathbf{T}^{-1}\mathbf{s}_i''.$$

We first average the M measurements taken by each GNSS receiver for each satellite, to obtain:

$$r_{n,i} = \frac{1}{M}\sum_{m=1}^{M} r_{n,i,m}.$$

Since under the Gaussian-noise assumption, $\{r_{n,i}\}$ are sufficient statistics for localization [51], we have the equivalent hypothesis test based on averaged measurements:

$$\mathcal{H}_0 : r_{n,i} = \left\| \mathbf{b}_0 + \mathbf{T}\mathbf{p}_{n_0} - \mathbf{s}_i \right\| + n_{n,i}, \tag{7}$$

$$\mathcal{H}_1 : r_{n,i} = \left\| \mathbf{p}_{n_0} + \mathbf{s}_i''' \right\| + \tau_i + n_{n,i}, \tag{8}$$

where $n_{n,i} = \frac{1}{M}\sum_{m=1}^{M} n_{n,i,m}$ is averaged noise with zero mean and variance $\frac{\sigma^2}{M}$. Averaging over the samples decreases $\frac{\sigma^2}{M}$ and improves the signal-to-noise ratio. Under $\mathcal{H}_0$, the rotation matrix $\mathbf{T}$ and the translation vector $\mathbf{b}_0$ are unknown, while under hypothesis $\mathcal{H}_1$, the vectors $\mathbf{s}_1''', ..., \mathbf{s}_I'''$, and $\tau_1, ..., \tau_I$ are unknown. In the next section, we devise a statistical test that can discriminate between $\mathcal{H}_0$ and $\mathcal{H}_1$.

3 Generalized likelihood ratio test for spoofer detection

We formulate a generalized likelihood ratio test (GLRT) to detect the presence of a spoofing attack. The GLRT compares the likelihoods of the data under $\mathcal{H}_0$ and $\mathcal{H}_1$, with all unknown parameters replaced by their maximum-likelihood estimates. The GLRT approach is appropriate for cases when there are unknown parameters under each hypothesis, and no prior knowledge of these parameters is available.

Since the measurements in (7) and (8) follow a normal distribution, and since all averaged noise samples are independent, the PDFs of the measurements under $\mathcal{H}_0$ and $\mathcal{H}_1$ are

$$p\left(\mathbf{r}; \mathbf{b}_0, \mathbf{T}, \mathcal{H}_0\right) = \frac{1}{\left(2\sigma^2 / M\right)^{\frac{NI}{2}}} e^{-\frac{\sum_{n=1}^{N}\sum_{i=1}^{I}\left(r_{n,i} - \left\|\mathbf{b}_0 + \mathbf{T}\mathbf{p}_{n_0} - \mathbf{s}_i\right\|\right)^2}{2\sigma^2/M}}, \tag{9}$$

and

$$p\left(\mathbf{r}; \mathbf{s}_1''', ..., \mathbf{s}_I''', \tau_1, ..., \tau_I, \mathcal{H}_1\right) = \frac{1}{\left(2\sigma^2 / M\right)^{\frac{NI}{2}}} e^{-\frac{\sum_{n=1}^{N}\sum_{i=1}^{I}\left(r_{n,i} - \left\|\mathbf{p}_{n_0} + \mathbf{s}_i'''\right\| - \tau_i\right)^2}{2\sigma^2/M}}. \tag{10}$$

The GLRT can be written as

$$\frac{\frac{1}{\left(2\sigma^2/M\right)^{\frac{NI}{2}}} e^{-\frac{\sum_{n=1}^{N}\sum_{i=1}^{I}\left(r_{n,i} - \left\|\mathbf{p}_{n_0} + \hat{\mathbf{s}}_i'''\right\| - \hat{\tau}_i\right)^2}{2\sigma^2/M}}}{\frac{1}{\left(2\sigma^2/M\right)^{\frac{NI}{2}}} e^{-\frac{\sum_{n=1}^{N}\sum_{i=1}^{I}\left(r_{n,i} - \left\|\hat{\mathbf{b}}_0 + \hat{\mathbf{T}}\mathbf{p}_{n_0} - \mathbf{s}_i\right\|\right)^2}{2\sigma^2/M}}} \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \gamma_{th}, \tag{11}$$

where

$$\left(\hat{\mathbf{b}}_0, \hat{\mathbf{T}}\right) = \arg\max p(\mathbf{r}; \mathbf{b}_0, \mathbf{T}, \mathcal{H}_0), \tag{12}$$

and

$$\left(\hat{\mathbf{s}}_i''', \hat{\tau}_i\right) = \arg\max p\left(\mathbf{r}; \mathbf{s}_i''', \tau_i, \mathcal{H}_1\right). \tag{13}$$

Taking the logarithm of (11) and simplifying yields

$$\sum_{n=1}^{N}\sum_{i=1}^{I}\left(r_{n,i} - f_0\left(\hat{\mathbf{b}}_0, \hat{\mathbf{T}}\right)\right)^2 - \sum_{n=1}^{N}\sum_{i=1}^{I}\left(r_{n,i} - f_1\left(\hat{\mathbf{s}}_i''', \hat{\tau}_i\right)\right)^2 \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \frac{2\sigma^2}{M}\ln\gamma_{th}, \tag{14}$$

where

$$f_0\left(\hat{\mathbf{b}}_0, \hat{\mathbf{T}}\right) = \left\|\hat{\mathbf{b}}_0 + \hat{\mathbf{T}}\mathbf{p}_n - \mathbf{s}_i\right\|,$$

and

$$f_1\left(\hat{\mathbf{s}}_i''', \hat{\tau}_i\right) = \left\|\mathbf{p}_{n_0} + \hat{\mathbf{s}}_i'''\right\| + \hat{\tau}_i.$$

As we see in (14), GLRT calculates the difference between the measurements and the best fit assuming that $\mathcal{H}_0$ and $\mathcal{H}_1$, respectively, are true.

4 Approximate parameter estimation

Evaluation of the GLRT requires the maximum-likelihood estimates of the parameters in (12) and (13). However, finding these estimates is a non-tractable problem. As a remedy, we resort to using the SR-LS technique [48] as a building block in an iterative algorithm. SR-LS was originally devised as a source localization method that finds the best position estimate (in a least squares sense) based on *squared* range measurements. We are going to use estimates from SR-LS here as a substitute for maximum-likelihood estimates required in (12) and (13). In this context, it is important to stress that under a Gaussian assumption on the measurement errors, SR-LS is asymptotically equivalent (for large numbers of samples, which

in our setting is equivalent to small σ^2/M) to maximum-likelihood. The range-squaring idea in [48] in ingenious and has also been used by other authors for joint position and orientation estimation of a rigid body from range measurements [52, 53].

4.1 Estimation of parameters under $\mathcal{H}_0$

Under $\mathcal{H}_0$, as an approximation to (12), we formulate the following problem, defined in terms of the squared range measurements:

$$\left(\widehat{\mathbf{b}}_0, \widehat{\mathbf{T}}\right) = \arg\min_{\mathbf{b}_0,\mathbf{T}} \sum_{n=1}^{N}\sum_{i=1}^{I}\left(\left\|\mathbf{b}_0+\mathbf{T}\mathbf{p}_{n_0}-\mathbf{s}_i\right\|^2 - r_{n,i}^2\right)^2, \tag{15}$$

We then solve (15) using cyclic optimization, alternating between minimization with respect to $\mathbf{b}_0$ and with respect to $\mathbf{T}$.

4.1.1 *Minimization of (15) with respect to* $\mathbf{b}_0$

Considering the rotation matrix $\mathbf{T}$ to be given, we first minimize (15) with respect to $\mathbf{b}_0$. Expanding the norm in (15) results in

$$\begin{aligned}\hat{\mathbf{b}}_0 = \arg\min_{\mathbf{b}_0} \sum_{n=1}^{N}\sum_{i=1}^{I}\Big(&\mathbf{b}_0^T\mathbf{b}_0 + \mathbf{b}_0^T\mathbf{T}\mathbf{p}_{n_0} - \mathbf{b}_0^T\mathbf{s}_i + \mathbf{p}_{n_0}^T\mathbf{T}^T\mathbf{b}_0 \\ &+\mathbf{p}_{n_0}^T\mathbf{T}^T\mathbf{T}\mathbf{p}_{n_0} - \mathbf{p}_{n_0}^T\mathbf{T}^T\mathbf{s}_i - \mathbf{s}_i^T\mathbf{b}_0 - \mathbf{s}_i^T\mathbf{T}\mathbf{p}_{n_0} + \mathbf{s}_i^T\mathbf{s}_i - r_{n,i}^2\Big)^2.\end{aligned} \tag{16}$$

Using the fact that $\mathbf{T}^T\mathbf{T} = \mathbf{I}$ and ordering (16) with respect to $\mathbf{b}_0$ yields

$$\begin{aligned}\hat{\mathbf{b}}_0 = \arg\min_{\mathbf{b}_0} \sum_{n=1}^{N}\sum_{i=1}^{I}\Big(&\mathbf{b}_0^T\mathbf{b}_0 + 2\left(\mathbf{T}\mathbf{p}_{n_0} - \mathbf{s}_i\right)^T\mathbf{b}_0 + \mathbf{p}_{n_0}^T\mathbf{p}_{n_0} \\ &-2\mathbf{p}_{n_0}^T\mathbf{T}^T\mathbf{s}_i + \mathbf{s}_i^T\mathbf{s}_i - r_{n,i}^2\Big)^2.\end{aligned} \tag{17}$$

To write (17) as squared norm, we introduce an auxiliary variable α and a constraint:

$$\begin{aligned}\hat{\mathbf{b}}_0 = \arg\min_{\mathbf{b}_0,\alpha\in R} \sum_{n=1}^{N}\sum_{i=1}^{I}\Big(&\alpha + 2\left(\mathbf{T}\mathbf{p}_{n_0} - \mathbf{s}_i\right)^T\mathbf{b}_0 + \mathbf{p}_{n_0}^T\mathbf{p}_{n_0} \\ &-2\mathbf{p}_{n_0}^T\mathbf{T}^T\mathbf{s}_i + \mathbf{s}_i^T\mathbf{s}_i - r_{n,i}^2\Big)^2 \\ \text{s.t. }\ &\mathbf{b}_0^T\mathbf{b}_0 = \alpha.\end{aligned} \tag{18}$$

The optimization problem in (18) can be written in a compact form as

$$\begin{aligned}\hat{\mathbf{b}}_0 = \arg\min_{\mathbf{y}}\ &\left\|\mathbf{A}\mathbf{y}-\mathbf{b}\right\|^2 \\ \text{s.t. }\ &\mathbf{y}^T\mathbf{D}\mathbf{y} + 2\mathbf{f}^T\mathbf{y} = 0,\end{aligned} \tag{19}$$

where

$$\mathbf{A} = \begin{bmatrix} 2\left(\mathbf{T}\mathbf{p}_{1_0} - \mathbf{s}_1\right)^T & 1 \\ \vdots & \vdots \\ 2\left(\mathbf{T}\mathbf{p}_{N_0} - \mathbf{s}_1\right)^T & 1 \\ 2\left(\mathbf{T}\mathbf{p}_{1_0} - \mathbf{s}_2\right)^T & 1 \\ \vdots & \vdots \\ 2\left(\mathbf{T}\mathbf{p}_{N_0} - \mathbf{s}_I\right)^T & 1 \end{bmatrix}, \quad \mathbf{y} = \begin{bmatrix} \mathbf{b}_0 \\ \alpha \end{bmatrix}, \tag{20}$$

$$\mathbf{b} = \begin{bmatrix} -\left(\mathbf{p}_{1_0}^T\mathbf{p}_{1_0} - 2\mathbf{p}_{1_0}^T\mathbf{T}^T\mathbf{s}_1 + \mathbf{s}_1^T\mathbf{s}_1 - r_{1,1}^2\right) \\ \vdots \\ -\left(\mathbf{p}_{N_0}^T\mathbf{p}_{N_0} - 2\mathbf{p}_{N_0}^T\mathbf{T}^T\mathbf{s}_1 + \mathbf{s}_1^T\mathbf{s}_1 - r_{N,1}^2\right) \\ -\left(\mathbf{p}_{1_0}^T\mathbf{p}_{1_0} - 2\mathbf{p}_{1_0}^T\mathbf{T}^T\mathbf{s}_2 + \mathbf{s}_2^T\mathbf{s}_2 - r_{1,1}^2\right) \\ \vdots \\ -\left(\mathbf{p}_{N_0}^T\mathbf{p}_{N_0} - 2\mathbf{p}_{N_0}^T\mathbf{T}^T\mathbf{s}_I + \mathbf{s}_I^T\mathbf{s}_I - r_{N,I}^2\right) \end{bmatrix}, \tag{21}$$

and

$$\mathbf{D} = \begin{bmatrix} \mathbf{I}_{2\times 2} & \mathbf{0}_{2\times 1} \\ \mathbf{0}_{1\times 2} & 0 \end{bmatrix}, \quad \mathbf{f} = \begin{bmatrix} \mathbf{0}_{2\times 1} \\ -0.5 \end{bmatrix}. \tag{22}$$

Note that $\mathbf{A}$ should have full column rank, i.e., $\mathbf{A}^T\mathbf{A}$ should be non-singular for the solution to exist. The optimization problem in (19) is non-convex. However, its global optimum solution can be found using the result in [54] as

$$\widehat{\mathbf{y}}(\lambda) = \left(\mathbf{A}^T\mathbf{A} + \lambda\mathbf{D}\right)^{-1}\left(\mathbf{A}^T\mathbf{b} - \lambda\mathbf{f}\right), \tag{23}$$

where λ is the unique solution of

$$\phi(\lambda) = 0, \lambda \in V, \tag{24}$$

and ϕ is defined as

$$\phi(\lambda) \triangleq \widehat{\mathbf{y}}(\lambda)\,\mathbf{D}\widehat{\mathbf{y}}(\lambda) + 2\mathbf{f}^T\widehat{\mathbf{y}}(\lambda). \tag{25}$$

The search interval for λ consists of the values for which the expression $\mathbf{A}^T\mathbf{A} + \lambda\mathbf{D}$ is positive definite. As a result, the search domain V will be

$$V = \left(-\frac{1}{\lambda_1\left(\mathbf{D}, \mathbf{A}^T\mathbf{A}\right)}, \infty\right). \tag{26}$$

Based on [54], the function $\phi(\lambda)$ is strictly decreasing over the domain V. Hence, we can use bisection to find the root of $\phi(\lambda)$.

4.1.2 *Minimization of (15) with respect to* $\mathbf{T}$

To minimize (15) with respect to the rotation matrix $\mathbf{T}$, for given $\mathbf{b}_0$, we again write, similarly to (17):

$$\begin{aligned}\widehat{\mathbf{T}} = \arg\min_{\mathbf{T}} \sum_{n=1}^{N}\sum_{i=1}^{I}\Big(&2\mathbf{b}_0^T\mathbf{T}\mathbf{p}_{n_0} - 2\mathbf{s}_i^T\mathbf{T}\mathbf{p}_{n_0} + \mathbf{p}_{n_0}^T\mathbf{p}_{n_0} \\ &+\mathbf{b}_0^T\mathbf{b}_0 - 2\mathbf{s}_i^T\mathbf{b}_0 + \mathbf{s}_i^T\mathbf{s}_i - r_{n,i}^2\Big)^2.\end{aligned} \tag{27}$$

Defining $c_{n,i} = \mathbf{p}_{n_0}^T \mathbf{p}_{n_0} + \mathbf{b}_0^T \mathbf{b}_0 - 2\mathbf{s}_i^T \mathbf{b}_0 + \mathbf{s}_i^T \mathbf{s}_i - r_{n,i}^2$ yields

$$\widehat{\mathbf{T}} = \arg\min_{\mathbf{T}} \sum_{n=1}^{N} \sum_{i=1}^{I} \left(2(\mathbf{b}_0 - \mathbf{s}_i)^T \mathbf{T} \mathbf{p}_{n_0} + c_{n,i} \right)^2. \quad (28)$$

Using the structure of the rotation matrix in (2) and defining $\mathbf{b}_0 - \mathbf{s}_i = [\, a_{i1}, a_{i2}]^T$ and $\mathbf{p}_{n_0} = [\, p_{n_{01}}, p_{n_{02}}]^T$, we can expand $2(\mathbf{b}_0 - \mathbf{s}_i)^T \mathbf{T} \mathbf{p}_{n_0}$ as

$$\begin{aligned} &2[\; a_{i1} \;\; a_{i2} \,] \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} p_{n_{01}} \\ p_{n_{02}} \end{bmatrix} \\ &= 2\left(p_{n_{01}} a_{i1} + p_{n_{02}} a_{i2} \right) \cos\theta + 2\left(p_{n_{01}} a_{i2} - p_{n_{02}} a_{i1} \right) \sin\theta \\ &= \alpha_{n,i} \cos\theta + \beta_{n,i} \sin\theta. \end{aligned} \quad (29)$$

Using (29), estimating $\mathbf{T}$ becomes equivalent to estimating θ as

$$f(\theta) = \arg\min_{\theta} \sum_{n=1}^{N} \sum_{i=1}^{I} \left(\alpha_{n,i} \cos\theta + \beta_{n,i} \sin\theta + c_{n,i} \right)^2. \quad (30)$$

Problem (30) is non-convex with respect to θ and may have multiple local minima. To find the global minimum, we calculate the derivative of (30) with respect to θ and find its roots. The derivative of the objective function in (30) is

$$\begin{aligned} f'(\theta) = &2 \sum_{n=1}^{N} \sum_{i=1}^{I} \left(-\alpha_{n,i} \sin\theta + \beta_{n,i} \cos\theta \right) \\ &\left(\alpha_{n,i} \cos\theta + \beta_{n,i} \sin\theta + c_{n,i} \right), \end{aligned} \quad (31)$$

which can be simplified into

$$\begin{aligned} f'(\theta) = &\sum_{n=1}^{N} \sum_{i=1}^{I} \left(\beta_{n,i}^2 - \alpha_{n,i}^2 \right) \sin\theta \cos\theta + \alpha_{n,i} \beta_{n,i} \left(2\cos^2\theta - 1 \right) \\ &- \alpha_{n,i} c_{n,i} \sin\theta + \beta_{n,i} c_{n,i} \cos\theta. \end{aligned} \quad (32)$$

Summation over the indexes n and i in (32) results in

$$f'(\theta) = e_1 \sin\theta \cos\theta + e_2 \left(2\cos^2\theta - 1 \right) + e_3 \sin\theta + e_4 \cos\theta, \quad (33)$$

with

$$\begin{aligned} e_1 &= \sum_{n=1}^{N} \sum_{i=1}^{I} \left(\beta_{n,i}^2 - \alpha_{n,i}^2 \right), \quad & e_2 &= \sum_{n=1}^{N} \sum_{i=1}^{I} \alpha_{n,i} \beta_{n,i}, \\ e_3 &= -\sum_{n=1}^{N} \sum_{i=1}^{I} \alpha_{n,i} c_{n,i}, & e_4 &= \sum_{n=1}^{N} \sum_{i=1}^{I} \beta_{n,i} c_{n,i}. \end{aligned} \quad (34)$$

The roots of f' in (33) are solutions to the equation

$$e_2 \left(2\cos^2\theta - 1 \right) + e_4 \cos\theta = -\left(e_1 \cos\theta + e_3 \right) \sin\theta. \quad (35)$$

We square both sides and substitute $\sin^2\theta = 1 - \cos^2\theta$ to obtain

$$\begin{aligned} &\left(e_1^2 + 4e_2^2 \right) \cos^4\theta + 2\left(e_1 e_3 + 2e_2 e_4 \right) \cos^3\theta \\ &+ \left(-e_1^2 - 4e_2^2 + e_4^2 + e_3^2 \right) \cos^2\theta \\ &+ \left(-2e_2 e_4 - 2e_1 e_3 \right) \cos\theta + e_2^2 - e_3^2 = 0, \end{aligned} \quad (36)$$

which is now a trigonometric function with only $\cos\theta$ terms (which are periodic with period 2π). Replacing $x = \cos\theta$ in (36) results in

$$\begin{aligned} &\left(e_1^2 + 4e_2^2 \right) x^4 + 2\left(e_1 e_3 + 2e_2 e_4 \right) x^3 \\ &+ \left(-e_1^2 - 4e_2^2 + e_3^2 + e_4^2 \right) x^2 \\ &- 2\left(e_1 e_3 + e_2 e_4 \right) x + e_2^2 - e_3^2 = 0. \end{aligned} \quad (37)$$

The fourth order equation in (37) has at most four roots, which can be found using the Ferrari's method [55]. After solving (37), we can use $\theta = \arccos x$ to find the values of θ corresponding to the local optimums of (30). Note that since $\cos\theta$ in (36) is periodic with period 2π, we look for the solutions in the domain $[0, 2\pi]$ when using $\theta = \arccos x$. The value of θ corresponding to the global optimum of (27), i.e., $\hat{\theta}$, is then

$$\hat{\theta} = \arg\min f(\theta_i). \quad (38)$$

4.1.3 *Iterative algorithm for minimization of (15)*

Minimizing (15) jointly with respect to $\mathbf{b}_0$ and θ (or equivalently, $\mathbf{T}$) is not tractable in closed form. Instead, we propose an iterative optimization approach in Algorithm 1. Since the problem is highly non-convex with multiple local optima, the point obtained as solution could depend on the initialization values (especially of θ). To tackle this, we repeat Algorithm 1 with different initial values of θ.

Algorithm 1 Iterative approach to minimization of (15) with respect to $\mathbf{b}_0$ and $\mathbf{T}$.

1: Pick an initial value for $\hat{\theta}$, denoted by $\hat{\theta}^0$;
2: Set $j = 0$;
3: Substitute $\hat{\theta}^j$ into (23) and get $\hat{\mathbf{b}}_0^j$;
4: Insert $\hat{\mathbf{b}}_0^j$ into (37) to obtain $\hat{\theta}^{j+1}$;
5: **if** $\left| \hat{\theta}^{j+1} - \hat{\theta}^j \right| \geq \varepsilon$ **then**
6: Set $j = j + 1$;
7: **Go to** 3;
8: **end if**

It is shown in [48] that the SR-LS results in the global optimum to the approximated problem based on squared range measurements. Hence, in the minimization with respect to $\mathbf{b}_0$, for given $\mathbf{T}$, in each iteration inside of Algorithm 1, we find the global optimum. The same is true of θ, as its global solution is given by the root of (37).

However, the overall problem is non-convex and the joint estimate of $\mathbf{b}_0$ and $\mathbf{T}$ may be suboptimal.

4.2 Estimation of parameters under $\mathcal{H}_1$

Next, to find approximate solutions to (13), we consider again a cyclic optimization algorithm that alternates between minimization with respect to $\mathbf{s}_1''', ..., \mathbf{s}_I'''$ and with respect to $\tau_1, ..., \tau_I$ and where SR-LS is used as a building block in the first-mentioned step.

4.2.1 Minimization with respect to $\mathbf{s}_1''', ..., \mathbf{s}_I'''$

We first consider minimization with respect to $\mathbf{s}_1''', ..., \mathbf{s}_I'''$ for given $\tau_1, ..., \tau_I$. Using the SR-LS technique, the corresponding optimization problem to find $\mathbf{s}_1''', ..., \mathbf{s}_I'''$ becomes

$$\left(\hat{\mathbf{s}}_1''', ..., \hat{\mathbf{s}}_I'''\right) = \arg \min_{\mathbf{s}_1''', ..., \mathbf{s}_I'''} \sum_{n=1}^{N} \sum_{i=1}^{I} \left(\left\| \mathbf{p}_{n_0} + \mathbf{s}_i''' \right\|^2 - \bar{r}_{n,i}^2 \right)^2, \tag{39}$$

where $\bar{r}_{n,i}^2 = \left(r_{n,i} - \tau_i\right)^2$. We expand the norm expression in (39) as

$$\left(\hat{\mathbf{s}}_1''', ..., \hat{\mathbf{s}}_I'''\right) = \arg \min_{\mathbf{s}_1''', ..., \mathbf{s}_I'''} \sum_{n=1}^{N} \sum_{i=1}^{I} \left(\mathbf{p}_{n_0}^T \mathbf{p}_{n_0} + 2\mathbf{p}_{n_0}^T \mathbf{s}_i''' + \left(\mathbf{s}_i'''\right)^T \mathbf{s}_i''' - \bar{r}_{n,i}^2 \right)^2, \tag{40}$$

and add the terms in (40) over index i to obtain

$$\begin{aligned} &\left(\hat{\mathbf{s}}_1''', ..., \hat{\mathbf{s}}_I'''\right) \\ &= \arg \min_{\mathbf{s}_1''', ..., \mathbf{s}_I'''} \sum_{n=1}^{N} \left(\left(\mathbf{s}_1'''\right)^T \mathbf{s}_1''' + 2\mathbf{p}_{n_0}^T \mathbf{s}_1''' + \mathbf{p}_{n_0}^T \mathbf{p}_{n_0} - \bar{r}_{n,1}^2 \right)^2 \\ &\quad + ... + \sum_{n=1}^{N} \left(\left(\mathbf{s}_I'''\right)^T \mathbf{s}_I''' + 2\mathbf{p}_{n_0}^T \mathbf{s}_I''' + \mathbf{p}_{n_0}^T \mathbf{p}_{n_0} - \bar{r}_{n,I}^2 \right)^2. \end{aligned} \tag{41}$$

Problem (41) is a minimization of sum of I positive terms, where the ith term only depends on $\mathbf{s}_i'''$. Hence, the problem decouples and we can minimize each individual term separately. This results in I separate optimization problems, where the ith problem is

$$\hat{\mathbf{s}}_i''' = \arg \min_{\mathbf{s}_i'''} \sum_{n=1}^{N} \left(\left(\mathbf{s}_i'''\right)^T \mathbf{s}_i''' + 2\mathbf{p}_{n_0}^T \mathbf{s}_i''' + \mathbf{p}_{n_0}^T \mathbf{p}_{n_0} - \bar{r}_{n,i}^2 \right)^2. \tag{42}$$

Similar to the approach in Section 4.1.1, moving the quadratic term to a constraint results in

$$\begin{aligned} \hat{\mathbf{s}}_i''' &= \arg \min_{\mathbf{s}_i''', \alpha \in R} \sum_{n=1}^{N} \left(\alpha + 2\mathbf{p}_{n_0}^T \mathbf{s}_i''' + \mathbf{p}_{n_0}^T \mathbf{p}_{n_0} - \bar{r}_{n,i}^2 \right)^2 \\ &\text{s.t. } \left(\mathbf{s}_i'''\right)^T \mathbf{s}_i''' = \alpha. \end{aligned} \tag{43}$$

By completing the square, we can cast (43) as

$$\begin{aligned} \hat{\mathbf{s}}_i''' &= \arg \min_{\mathbf{y}} \left\| \mathbf{A}\mathbf{y} - \mathbf{b} \right\|^2 \\ &\text{s.t. } \mathbf{y}^T \mathbf{D} \mathbf{y} + 2\mathbf{f}^T \mathbf{y} = 0, \end{aligned} \tag{44}$$

where

$$\mathbf{A} = \begin{bmatrix} 2\mathbf{p}_{1_0}^T & 1 \\ . & . \\ 2\mathbf{p}_{N_0}^T & 1 \end{bmatrix}, \mathbf{b} = \begin{bmatrix} \bar{r}_{1,i}^2 - \mathbf{p}_1^T \mathbf{p}_1 \\ . \\ \bar{r}_{N,i}^2 - \mathbf{p}_{N_0}^T \mathbf{p}_{N_0}, \end{bmatrix}, \tag{45}$$

and

$$\mathbf{y} = \begin{bmatrix} \mathbf{s}_i''' \\ \alpha \end{bmatrix}, \mathbf{D} = \begin{bmatrix} \mathbf{I}_2 & \mathbf{0}_{1\times 2} \\ \mathbf{0}_{1\times 2} & 0 \end{bmatrix}, \mathbf{f} = \begin{bmatrix} \mathbf{0} \\ -0.5 \end{bmatrix}. \tag{46}$$

4.2.2 Minimization with respect to τ_i

Next, we find the artificial time delays caused by each spoofer for given values of $\mathbf{s}_1''', ..., \mathbf{s}_I'''$. The problem is

$$(\widehat{\tau}_1, ..., \widehat{\tau}_I) = \arg \min_{\tau_1, ..., \tau_I} \sum_{n=1}^{N} \sum_{i=1}^{I} \left(\left\| \mathbf{p}_{n_0} + \mathbf{s}_i''' \right\| + \tau_i - r_{n,i} \right)^2. \tag{47}$$

We expand (47) as

$$\begin{aligned} (\widehat{\tau}_1, ..., \widehat{\tau}_I) &= \arg \min_{\tau_1, ..., \tau_I} \sum_{n=1}^{N} \left(\left\| \mathbf{p}_{n_0} + \mathbf{s}_1''' \right\| + \tau_1 - r_{n,1} \right)^2 \\ &\quad + ... + \sum_{n=1}^{N} \left(\left\| \mathbf{p}_{n_0} + \mathbf{s}_I''' \right\| + \tau_I - r_{n,I} \right)^2. \end{aligned} \tag{48}$$

The objective function in (48) is sum of positive and independent terms. Again, the problem decouples and we can find the minima with respect to $\tau_1, ..., \tau_I$ separately for $i = 1, ..., I$. The corresponding problem for the ith variable, τ_i, is

$$\widehat{\tau}_i = \arg \min_{\tau_i} \sum_{n=1}^{N} \left(\left\| \mathbf{p}_{n_0} + \mathbf{s}_i''' \right\| + \tau_i - r_{n,i} \right)^2. \tag{49}$$

and has the (s) solution

$$\tau_i = \frac{\sum_{n=1}^{N} r_{n,i} - \left\| \mathbf{p}_{n_0} + \mathbf{s}_i''' \right\|}{N}. \tag{50}$$

4.2.3 Iterative algorithm for approximate solution of (13)

The whole approach to estimate the parameters under $\mathcal{H}_1$ is summarized in Algorithm 2. Since the estimation problem is non-linear and can have multiple local optimum points, we need to repeat Algorithm 2 for different initialization points of $\tau_1, ..., \tau_I$.

Similarly to the case under $\mathcal{H}_1$, the minimization with respect to $\mathbf{s}_1''', ..., \mathbf{s}_I'''$ for given $\tau_1, ..., \tau_I$ in Algorithm 2 returns the global optimum. Also, for given $\mathbf{s}_1''', ..., \mathbf{s}_I'''$, (50) yields the globally optimal values of $\tau_1, ..., \tau_I$. However,

the joint estimates $\mathbf{s}_1^{'''}, ..., \mathbf{s}_I^{'''}$ and $\tau_1, ..., \tau_I$ delivered by Algorithm 2 may be suboptimal. A more granular initialization range for the parameter θ increases the chance of finding the global optimum rather than a local optimum.

Algorithm 2 Iterative approach to approximation of $\mathbf{s}_1^{'''}, ..., \mathbf{s}_I^{'''}$ and $\tau_1, ..., \tau_I$ in (13).

1: Pick initial values for $\widehat{\tau}_1, ..., \widehat{\tau}_I$ denoted by $\widehat{\boldsymbol{\tau}}^0 = [\widehat{\tau}_1^0, ..., \widehat{\tau}_I^0]$;
2: Set $j = 0$;
3: Substitute $\widehat{\tau}_i^j$ in (44) to get $\widehat{\mathbf{s}}_i^{j'''}$ for $i = 1, ..., I$;
4: Insert $\widehat{\mathbf{s}}_i^{j'''}$ into (50) to obtain $\widehat{\tau}_i^{j+1}$ for $i = 1, ..., I$;
Defining $d^j = \sum_{n=1}^{N} \sum_{i=1}^{I} \left[r_{n,i} - \left(\left\| \mathbf{p}_{n_0} + \mathbf{s}_i^{j'''} \right\| + \tau_i^j \right) \right]^2$,
5: **if** $\left| d^j - d^{j+1} \right| \geq \epsilon$ **then**
6: Set $j = j + 1$;
7: **Go to** 3;
8: **end if**

4.3 Complexity analysis of the proposed algorithms

In this section, we provide the Big-O complexity for each step of Algorithms 1 and 2, respectively. Algorithm 1 is comprised of two parts where $\mathbf{b}_0$ is first estimated using (23) and θ is estimated using (37), which is solved using Ferrari's method. Adding up the complexity of these two parts, the complexity of each iteration of Algorithm 1 is:

$$4O(3NI) + O(9NI) + O\left(\log_2(r)\right), \tag{51}$$

where $r = \log_2\left(\frac{\varepsilon_0}{\varepsilon}\right)$, ε_0 is the search domain of the bisection algorithm in (26), and ε is the required accuracy of the bisection algorithm. The overall complexity of (51) is the number of tested initial values of θ_0 multiplied by the complexity of each iteration provided in (51).

Similarly, Algorithm 2 is comprised of two parts. First, the values of $\mathbf{s}_1^{'''}, ..., \mathbf{s}_I^{'''}$ are estimated and then $\tau_1, ..., \tau_I$ are computed. Adding the complexity of these two parts, the complexity of each iteration of Algorithm 1 is:

$$I \times \left[4O(3N) + O(9N) + O\left(\log_2(r)\right)\right] \tag{52}$$

5 Optimal design of attack parameters

As we develop signal processing methodology to detect an attack by multiple spoofers, it is expected that the adversary devises the best strategy to counteract the spoofing detection technique. In this section, we develop analytical solutions to design the optimal spoofing parameters. In this analysis, we assume that the adversary has perfect knowledge of the initial positions of the GNSS receiver nodes, $\mathbf{p}_{n_0}$.

To minimize the chance of detection, the adversary needs to satisfy two types of constraints. First, the adversary needs to find spoofed locations, $\mathbf{p}_n^{sp}$, such that the relative coordinates of the GNSS receivers is preserved after spoofing. To achieve this, the spoofer selects values of the spoofed translation vector, $\mathbf{b}_0^{sp}$, and spoofed rotation matrix, $\mathbf{T}^{sp}$. Then, it uses the knowledge of $\mathbf{p}_{n_0}$ to calculate the values of the spoofed locations, $\mathbf{p}_n^{sp}$, as

$$\mathbf{p}_n^{sp} = \mathbf{b}_0^{sp} + \mathbf{T}^{sp}\mathbf{p}_{n_0}. \tag{53}$$

Second, the locations of the spoofers and forged positions of the satellites need to chosen such that the range measurements at all GNSS receivers result in the target spoofed location derived in (53), and the spoofed formation of the GNSS receivers is preserved. To satisfy this, the simulated distance by a specific spoofer, caused by its physical distance to a GNSS receiver and artificial delay, needs to be equal to the distance of forged satellite, provided in the simulated GNSS signal, to the estimated position of that GNSS receiver. To implement the former in the best way, the adversary first picks values for the forged positions of the satellites, $\mathbf{s}_i^{sp}$, and uses the values of $\mathbf{p}_n^{sp}$ derived in (53) to satisfy the following constrains:

$$\left\| \mathbf{p}_i^A - \mathbf{p}_n \right\| + \tau_i = \left\| \mathbf{p}_n^{sp} - \mathbf{s}_i^{sp} \right\|, \tag{54}$$

where $\mathbf{p}_i^A$ is the position of the ith spoofer, $\mathbf{p}_n^{sp}$ is the spoofed location of the nth GNSS receiver, $\mathbf{s}_i^{sp}$ is the forged position of the ith satellite, and τ_i is the artificial delay produced by the ith spoofer. The better the spoofers satisfy the corresponding equations in (54), the closer the estimated parameters in (3) to that set by the adversary. Consequently, this leads to a better fit between the measurements and the data model. As we see in the developed detection test in (14), this helps reducing the left hand side of the detection test and not reaching the detection threshold.

Each spoofer chooses values for $\mathbf{s}_i^{sp}$ since these values need to be in a specific range, e.g., GEO satellites, and then solves the related equations in (54) to get the optimal values of $\mathbf{p}_i^A$ and τ_i. To illustrate, the best position for the first attacker is illustrated in Fig. 2 for $N = I = A = 2$. As we see, satisfying the set of constraints in (54) results in the optimal position for the spoofer being the intersection of two circles where the center of each circle is $\mathbf{p}_n$ for $n = 1, 2$. For $N \geq 3$, there are three circles which may not have a common intersection point. Therefore, the adversary needs to find the best point for each spoofer which best satisfies (54) for all GNSS receivers. One way is to use a least squares fit,

$$\min \sum_{n=1}^{N} \left[\left\| \mathbf{p}_i^A - \mathbf{p}_n^{sp} \right\|^2 - \left(\mu_{n,i} - \tau_i \right)^2 \right]^2, \tag{55}$$

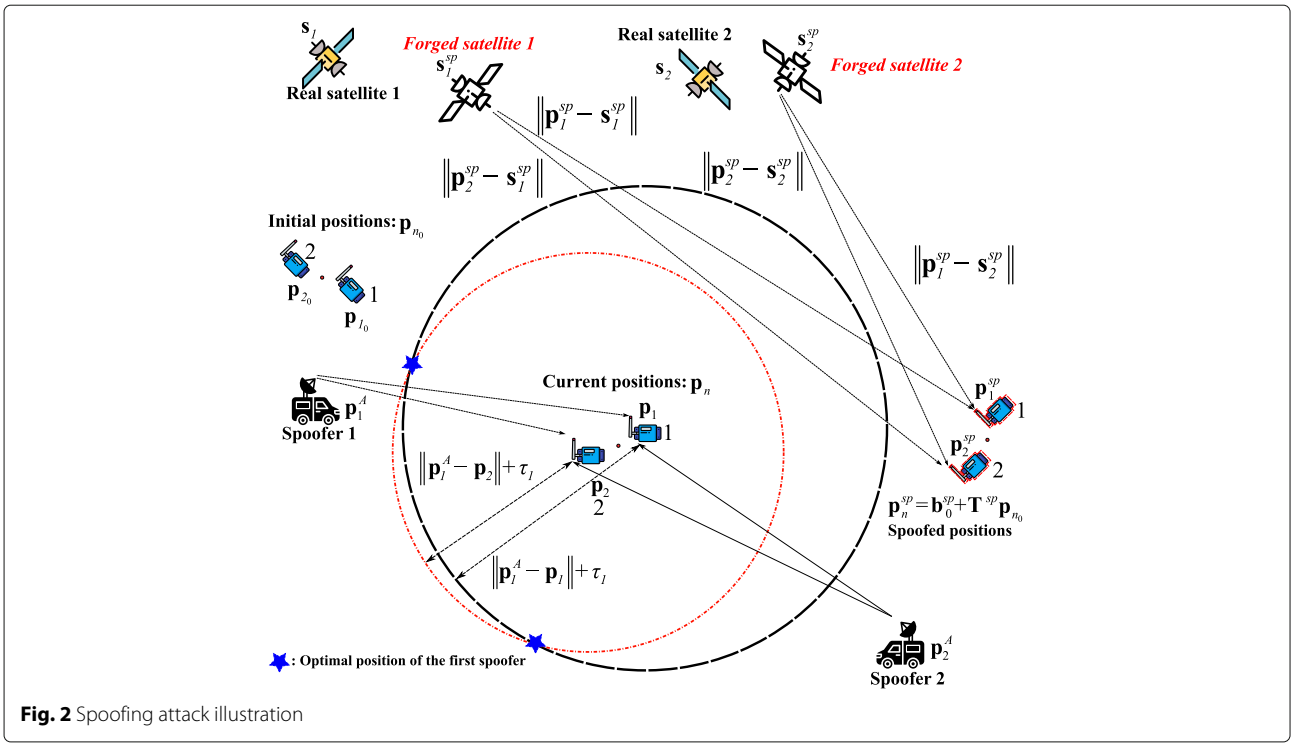

Fig. 2 Spoofing attack illustration

where $\mu_{n,i} = \left\|\mathbf{p}_n^{sp} - \mathbf{s}_i^{sp}\right\|$. To solve (55), we do the following change of variables:

$$\mathbf{p}_n = \begin{bmatrix} p_{n_x} \\ p_{n_y} \end{bmatrix}, \quad \mathbf{p}_i^A = \begin{bmatrix} x_i \\ y_i \end{bmatrix}, \tag{56}$$

and calculate the derivatives of the objective in (55) with respect to p_{n_x}, p_{n_y}, and τ_i. After algebraic simplifications, we get

$$\begin{aligned}
\frac{\partial f}{\partial x_i} =& N x_i^3 - 3\sum_{n=1}^{N} p_{n_x} x_i^2 + \left(3\sum_{n=1}^{N}\left(p_{n_x}\right)^2 + \sum_{n=1}^{N} c_{n,i}\right) x_i \\
&+ \sum_{n=1}^{N}\left(-\left(p_{n_x}\right)^3 - p_{n_x} c_{n,i}\right), \\
\frac{\partial f}{\partial y_i} =& N y_i^3 - 3\sum_{n=1}^{N} p_{n_y} y_i^2 + \left(3\sum_{n=1}^{N}\left(p_{n_y}\right)^2 + \sum_{n=1}^{N} d_{n,i}\right) y_i \\
&+ \sum_{n=1}^{N}\left(-\left(p_{n_y}\right)^3 - p_{n_y} d_{n,i}\right), \\
\frac{\partial f}{\partial \tau_i} =& N \tau_i^3 - 3\sum_{n=1}^{N} \mu_{n,i} \tau_i^2 + \sum_{n=1}^{N}\left(3\mu_{n,i}^2 - e_{n,i}\right) \tau_i \\
&+ \sum_{n=1}^{N} -\mu_{n,i}^3 + \mu_{n,i} e_{n,i},
\end{aligned} \tag{57}$$

where

$$\begin{aligned}
c_{n,i} &= \left(y_i - p_{n_y}\right)^2 - \left(\mu_{n,i} - \tau_i\right)^2, \\
d_{n,i} &= \left(x_i - p_{n_x}\right)^2 - \left(\mu_{n,i} - \tau_i\right)^2, \\
e_{n,i} &= \left(x_i - p_{n_x}\right)^2 + \left(y_i - p_{n_y}\right)^2.
\end{aligned} \tag{58}$$

Relations (58) imply an intertwined system of non-linear equations in (57). This system of equations can be solved using classic approaches such as the Newton method. To find the optimal values of $\mathbf{p}_i^A$ and τ_i for each spoofer, we perform a coarse search over multiple initial guess points and choose the best one among them.

Nonetheless, in practice, it may not be possible for each spoofer to be in the optimal location at each moment. This is due to the fact that the GNSS receivers are installed on a moving platform and physical barriers as well as unknown velocity and speed can prevent the spoofers from being at the required positions. We quantify the spoofing detection performance with respect to the deviation from the optimal location of the spoofers in Section 6.

6 Simulation results

In this section, we present numerical examples to quantify the performance of the proposed spoofing detection mechanism. Unless otherwise stated, the parameters of the simulation setup are as in Table 2.

To initialize $\hat{\theta}$ for Algorithm 1, we select a set of coarsely spaced values within the range $[0, 2\pi]$. We repeat Algorithm 2 for different initial values of $\tau_1, ..., \tau_I$ and then

Table 2 Simulations parameters for the spoofing scenario

Parameter	Value
GNSS initial positions, $\mathbf{p}_{n_0}$ for $N = 3$	[(10, 30), (20, − 60), (− 10, 40)]
GNSS initial positions, $\mathbf{p}_{n_0}$ for $N = 5$	[(10, 30), (20, − 60), (− 10, 40), (− 5, − 6), (7, 5)]
Satellite positions	10^6[(− 7, 36.786), (− 3, 35), (5, − 35.5)]
Rotation angle, θ	7π / 6
Translation vector, $\mathbf{b}_0$	[12 , 4]
Spoofer positions for $\mathbf{b}_0^{sp} = 10^3$[0.5,0.5]	10^4[(1.7534, 0.1163), (− 0.6936, 0.9408), (− 1.2268, −0.1218)]
Artificial time delays for $\mathbf{b}_0^{sp} = 10^3$[0.5,0.5]	10^7(3.7388, 3.5156, 3.4883)
Spoofer positions for $\mathbf{b}_0^{sp} = 10^3$[5,5]	10^4[(1.7534, 0.1163), (− 0.6936, 0.9408), (− 1.2268, − 0.1218)]
Artificial time delays for $\mathbf{b}_0^{sp} = 10^3$[5,5]	10^7[(3.73, 3.51, 3.48)]
Noise power, σ^2	2×10^3

All the distances and locations are in meters

pick the estimated parameters which result in the least difference between the measurements and the data model. The values of ϵ in both Algorithms 1 and 2 are set to $\epsilon = 10^{-3}$.

To demonstrate the accuracy of the parameter estimates used in lieu of the maximum-likelihood estimates required in (12)–(13), we first compare the empirical estimation variance to the Cramér-Rao lower bound (CRLB). The CRLBs under $\mathcal{H}_0$ and $\mathcal{H}_1$ are derived in Appendix A and Appendix B, respectively. Due to space constraints, we present these comparisons only for the parameters θ for $\mathcal{H}_0$ and s_{31}''' for $\mathcal{H}_1$. Figures 3 and 4 show the results. As we can see, parameter estimates get close to their respective CRLBs as the noise variances decrease.

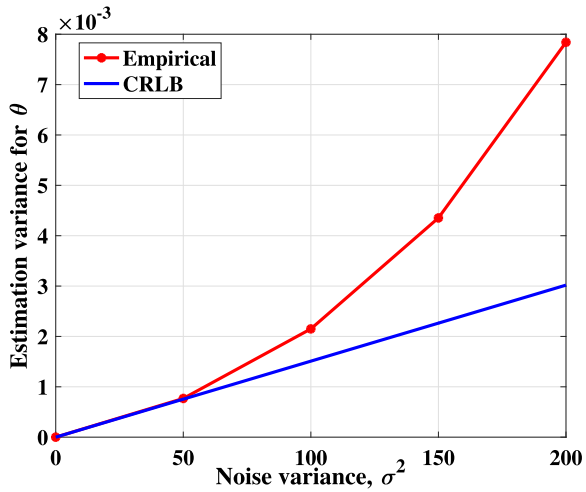

Fig. 3 Estimation variance for θ as function of the noise power σ^2, compared to the CRLB

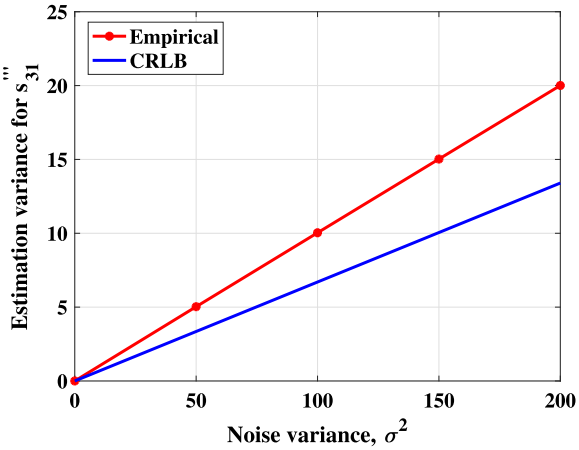

Fig. 4 Estimation variance for s_{31}''' as function of the noise power σ^2, compared to the CRLB

We next evaluate the performance of the proposed spoofing detection technique by plotting the probability of detection versus the probability of false alarm for various different values of M (or equivalently, different noise power $\frac{\sigma^2}{M}$ in the averaged range measurements). To generate the simulation results and find the threshold of the GLRT, we proceed as follows. First, we run a case without spoofers and empirically calculate the probability of false alarm using the GLRT test in (14) for various values of γ_{th}. Next, we simulate the presence of spoofers and calculate the probability of detection using the GLRT test in (14) for various values of γ_{th}. Finally, we plot the so-obtained probabilities of detection and false alarm.

In the first simulation scenario, we investigate how the difference between the true and spoofed positions of the GNSS receivers affect the spoofing detection probability. We present the probability of detection versus false alarm in Figs. 5 and 6 for different values of the spoofed trans-

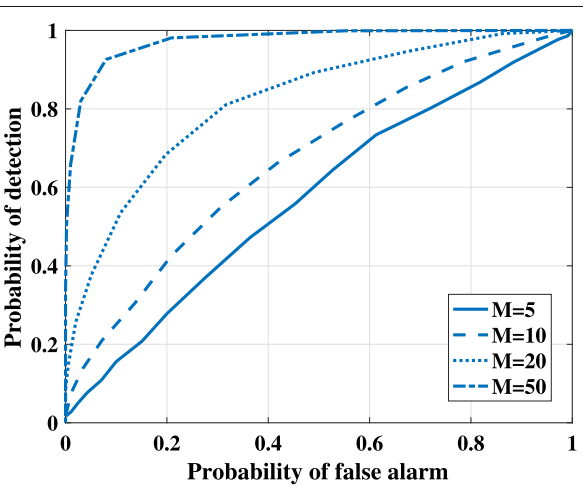

Fig. 5 Probability of detection versus probability of false alarm for $N = l = 3$ and $b_0^{sp} = 10^3 \times [0.5, 0.5]$

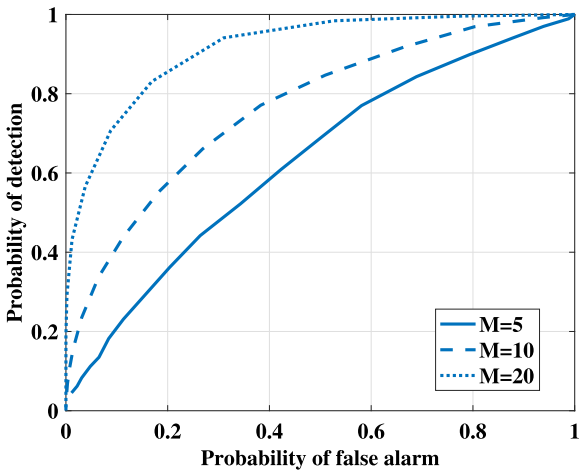

Fig. 6 Probability of detection versus probability of false alarm for $N = I = 3$ and $b_0^{sp} = 10^3 \times [5, 5]$

lation vector, $\mathbf{b}_0^{sp}$. The results show that as the adversary tries to mislead the victims more from their true locations, the chance to spot the spoofing attack increases.

In the next scenario, we quantify the performance of the proposed technique when the position of each spoofer deviates from the optimal designed positions. The probability of detection versus false alarm is shown in Fig. 7 when each spoofer is moved by $2\mathbf{p}_i^A / \|\mathbf{p}_i^A\|$ from the optimal position. As we see, the probability of detection increases as the spoofers fail to occupy their optimal locations.

Finally, we investigate the effect of the number of GNSS receivers on the performance of the proposed algorithm. We consider the same satellite formation with $I = 3$ and three spoofers, i.e., $A = 3$, while increasing the number of GNSS receivers from three to five. The performance of the proposed algorithm when increasing the number of GNSS receivers is shown in Fig. 8. Compared to Fig. 5, we see that adding two extra GNSS receivers increases the detection performance of the proposed scheme considerably.

As we see in Figs. 5-8, increasing the number of samples taken by the GNSS receivers consistently increases the detection probability for a given false alarm probability.

7 Conclusions

We proposed an anti-spoofing approach for GNSS based on a statistical test. The test exploits multiple GNSS receivers mounted on a rigid-body platform (with a priori unknown position and orientation) and essentially performs a consistency check between all pairs of measured receiver-satellite distances and available prior knowledge about the relative positions of the receivers on the platform. Numerical simulations proved the feasibility of our method and specifically showed that the more the spoofers try to manipulate the estimated GNSS receiver positions from their nominal locations, the higher is the probability of attack detection. Also, the more GNSS receivers on the platform, the higher the probability of detecting a spoofing attack.

We furthermore showed that using multiple GNSS receivers limits the feasible attacker position to few locations, and we designed a framework for finding the optimal attack positions as well as the artificial time delays of the spoofers. Simulations showed that when the spoofers do not occupy their optimal locations, it is easier to detect them.

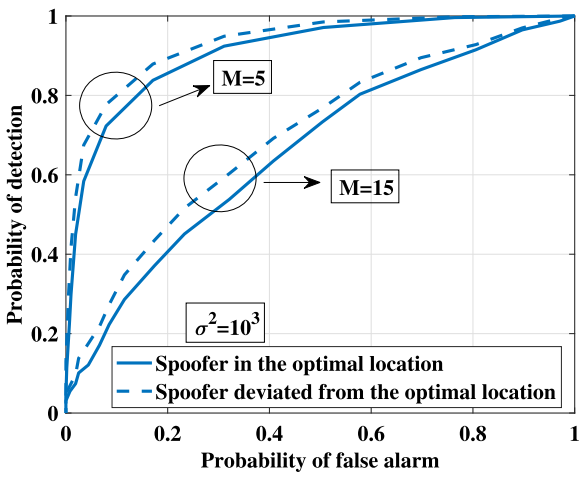

Fig. 7 Probability of detection versus probability of false alarm for $N = I = 3$ and $\mathbf{b}_0^{sp} = 10^3 \times [0.5, 0.5]$ when the spoofer locations deviate by $\frac{2\mathbf{p}_i^A}{\|\mathbf{p}_i^A\|}$

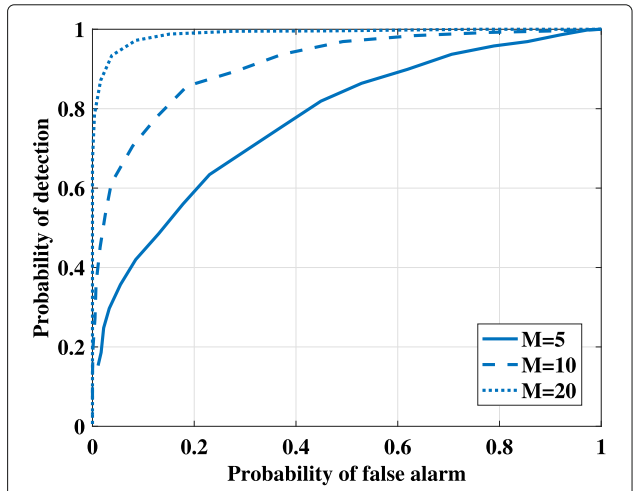

Fig. 8 Probability of detection versus probability of false alarm for $N = 5$ and $I = 3$ and $\mathbf{b}_0^{sp} = 10^3 \times [0.5, 0.5]$

For analytical tractability and to achieve a first proof-of-concept of our statistical test methodology, we considered a two-dimensional geometry. Future work may include extensions to a three-dimensional world or combining our approach with anomaly detection in the autocorrelation function of the received signals, in order to enhance overall detection performance. In addition, new analysis can be performed by considering synchronization errors among the clocks of the GNSS receivers and the satellites. Also, the noise variance may be treated as an unknown parameter in the GLR tests.

It would be interesting to test our proposed approach in practice. We hope that this paper will stimulate both further theoretical research and experimental work.

Appendix A

Proof of CRLB for $\mathcal{H}_0$

In this appendix, we calculate the CRLB for estimated parameters under hypothesis $\mathcal{H}_0$. Since the range measurements in (5) follow a normal distribution, we can use the Slepian-Bang formula [56] to calculate the CRLB as,

$$[\mathbf{I}(\boldsymbol{\alpha})]_{jk} = \left[\frac{\partial \boldsymbol{\mu}(\boldsymbol{\alpha})}{\partial \alpha_j}\right]^T \mathbf{C}^{-1}(\boldsymbol{\alpha}) \left[\frac{\partial \boldsymbol{\mu}(\boldsymbol{\alpha})}{\partial \alpha_k}\right], \tag{59}$$

where

$$\begin{aligned} \boldsymbol{\alpha} &= [b_{01}, b_{02}, \theta]^T, \\ [\mu(\boldsymbol{\alpha})]_{n,i,m} &= \left\| \mathbf{b}_0 + \mathbf{T}\mathbf{p}_{n_0} - \mathbf{s}_i \right\|, \\ \frac{\partial \mu(\boldsymbol{\alpha})}{\partial \alpha_j} &= \left[\frac{\partial [\mu(\boldsymbol{\alpha})]_1}{\partial \alpha_j}, \frac{\partial [\mu(\boldsymbol{\alpha})]_2}{\partial \alpha_j}, ..., \frac{\partial [\mu(\boldsymbol{\alpha})]_{NIM}}{\partial \alpha_j} \right]^T, \end{aligned} \tag{60}$$

and $\mathbf{C}^{-1}(\boldsymbol{\alpha}) = \sigma^{-2}$ since the noises across the GNSS receivers and the measurements are assumed to be independent.

To calculate the CRLB for $\mathcal{H}_0$, first, we calculate the values of $\frac{\partial \mu(\boldsymbol{\alpha})}{\partial \alpha_j}$ for $j = 1, 2, 3$. After some algebraic calculations, these values are derived as

$$\begin{aligned} \frac{\partial [\mu(\boldsymbol{\alpha})]_{n,i,m}}{\partial b_{01}} &= \frac{b_{01} + p_{n1}\cos\theta - p_{n2}\sin\theta - s_{i1}}{\left\| \mathbf{b}_0 + \mathbf{T}\mathbf{p}_{n_0} - \mathbf{s}_i \right\|}, \\ \frac{\partial [\mu(\boldsymbol{\alpha})]_{n,i,m}}{\partial b_{02}} &= \frac{b_{02} + p_{n1}\sin\theta + p_{n2}\cos\theta - s_{i2}}{\left\| \mathbf{b}_0 + \mathbf{T}\mathbf{p}_{n_0} - \mathbf{s}_i \right\|}, \\ \frac{\partial [\mu(\boldsymbol{\alpha})]_{n,i,m}}{\partial \theta} &= \frac{A_{n,i}\cos\theta + B_{n,i}\sin\theta}{\left\| \mathbf{b}_0 + \mathbf{T}\mathbf{p}_{n_0} - \mathbf{s}_i \right\|}, \end{aligned} \tag{61}$$

where

$$\begin{aligned} A_{n,i} &= b_{02}p_{n1} - b_{01}p_{n2} - s_{i2}p_{n1} + s_{i1}p_{n2}, \\ B_{n,i} &= -b_{02}p_{n2} - b_{01}p_{n1} + s_{i1}p_{n1} + s_{i2}p_{n2}. \end{aligned} \tag{62}$$

By inserting the calculated values of (61) into the Slepian-Bang formula in (59), the elements of the Fisher information matrix are derived as

$$\begin{aligned} [\mathbf{I}(\boldsymbol{\alpha})]_{11} =& M \sum_{n=1}^{N}\sum_{i=1}^{I} \frac{(b_{01} + p_{n1}\cos\theta - p_{n2}\sin\theta - s_{i1})^2}{\left\| \mathbf{b}_0 + \mathbf{T}\mathbf{p}_{n_0} - \mathbf{s}_i \right\|^2}, \\ [\mathbf{I}(\boldsymbol{\alpha})]_{12} =& M \sum_{n=1}^{N}\sum_{i=1}^{I} \frac{(b_{01} + p_{n1}\cos\theta - p_{n2}\sin\theta - s_{i1})}{\left\| \mathbf{b}_0 + \mathbf{T}\mathbf{p}_{n_0} - \mathbf{s}_i \right\|^2} \\ & \times (b_{02} + p_{n1}\sin\theta + p_{n2}\cos\theta - s_{i2}), \\ [\mathbf{I}(\boldsymbol{\alpha})]_{13} =& M \sum_{n=1}^{N}\sum_{i=1}^{I} \frac{(b_{01} + p_{n1}\cos\theta - p_{n2}\sin\theta - s_{i1})}{\left\| \mathbf{b}_0 + \mathbf{T}\mathbf{p}_{n_0} - \mathbf{s}_i \right\|^2} \\ & \times (A_{n,i}\cos\theta + B_{n,i}\sin\theta), \\ [\mathbf{I}(\boldsymbol{\alpha})]_{22} =& M \sum_{n=1}^{N}\sum_{i=1}^{I} \frac{(b_{02} + p_{n1}\sin\theta + p_{n2}\cos\theta - s_{i2})^2}{\left\| \mathbf{b}_0 + \mathbf{T}\mathbf{p}_{n_0} - \mathbf{s}_i \right\|^2}, \\ [\mathbf{I}(\boldsymbol{\alpha})]_{23} =& M \sum_{n=1}^{N}\sum_{i=1}^{I} \frac{(b_{02} + p_{n1}\sin\theta + p_{n2}\cos\theta - s_{i2})}{\left\| \mathbf{b}_0 + \mathbf{T}\mathbf{p}_{n_0} - \mathbf{s}_i \right\|^2} \\ & \times (A_{n,i}\cos\theta + B_{n,i}\sin\theta), \\ [\mathbf{I}(\boldsymbol{\alpha})]_{33} =& M \sum_{n=1}^{N}\sum_{i=1}^{I} \frac{(A_{n,i}\cos\theta + B_{n,i}\sin\theta)^2}{\left\| \mathbf{b}_0 + \mathbf{T}\mathbf{p}_{n_0} - \mathbf{s}_i \right\|^2}, \end{aligned} \tag{63}$$

and $[\mathbf{I}(\boldsymbol{\alpha})]_{21} = [\mathbf{I}(\boldsymbol{\alpha})]_{12}$, $[\mathbf{I}(\boldsymbol{\alpha})]_{31} = [\mathbf{I}(\boldsymbol{\alpha})]_{13}$, $[\mathbf{I}(\boldsymbol{\alpha})]_{32} = [\mathbf{I}(\boldsymbol{\alpha})]_{23}$. Using the calculated elements of the Fisher matrix, we can derive closed-form expressions for the CRLB by inverting the Fisher information matrix. For the sake of conciseness, here, we avoid showing these expressions.

Appendix B

Proof of CRLB for $\mathcal{H}_1$

In this appendix, we calculate the CRLB for the parameters under hypothesis $\mathcal{H}_1$. Since the range measurements in (5) follow a normal distribution, we can use the Slepian-Bang formula [56] to calculate the CRLB.

Based on Algorithm 2, the first step is to find initial values of the parameters τ_i for $i = 1, .., I$. As we see in (45), estimation of $\mathbf{s}_i'''$ depends on $\bar{r}_{n,i}^2$ for $n = 1, ..., N$ where $\bar{r}_{n,i}^2$ depends on τ_i for $n = 1, ..., N$. Hence, only τ_i is used in (43) to estimate $\mathbf{s}_i'''$ for $i = 1, ...I$.

In the next step of Algorithm 2, calculated values of $\mathbf{s}_i'''$ are used to estimate τ_i for $i = 1, .., I$. Based on (50), only $\mathbf{s}_i'''$ is used to estimate τ_i for $i = 1, .., I$. According to the previous explanations, each pair $(\mathbf{s}_i''', \tau_i)$ is estimated independently for $i = 1, ..., I$. In the following, we provide the details to calculate the CRLB for $\mathcal{H}_1$.

Similar to the calculations for $\mathcal{H}_0$, we use the Slepian-Bang relation (59) to calculate the CRLB for $\mathcal{H}_1$. The problem parameters and the mean of the hypothesis are defined as

$$\begin{aligned}\boldsymbol{\alpha} &= \left[s_{11}^{'''}, s_{12}^{'''}, \tau_1, ..., s_{I1}^{'''}, s_{I2}^{'''}, \tau_I\right],\\ [\mu(\boldsymbol{\alpha})]_{n,i} &= \left\|\mathbf{p}_{n_0} + \mathbf{s}_i^{'''}\right\| + \tau_i,\end{aligned} \tag{64}$$

and $\mathbf{C}^{-1}(\boldsymbol{\alpha}) = \sigma^{-2}$ since the noises across the GNSS receivers and the measurements are assumed to be independent. As we see, $\boldsymbol{\alpha}$ depends on different parameters of one specific satellite for each value of i. To avoid confusion, we can assume that for $[\mu(\boldsymbol{\alpha})]_{n,i}$ the parameters with index $i = 1, ..., i-1, i+1, ..., I$ have coefficient zero. Hence, the FIM will be block diagonal and each block is 3×3 since three parameters from each satellite need to be estimated. Considering that M samples are captured from the same satellite by the same GNSS receiver, we factor out M.

The derivative of $[\mu(\boldsymbol{\alpha})]_{n,i}$ with respect to the parameters related to the ith satellite are defined as

$$\begin{aligned}\frac{[\mu(\boldsymbol{\alpha})]_{n,i}}{\partial s_{i1}^{'''}} &= \frac{p_{n_{01}} + s_{i1}^{'''}}{\left\|\mathbf{p}_{n_0} + \mathbf{s}_i^{'''}\right\|},\\ \frac{[\mu(\boldsymbol{\alpha})]_{n,i}}{\partial s_{i2}^{'''}} &= \frac{p_{n_{02}} + s_{i2}^{'''}}{\left\|\mathbf{p}_{n_0} + \mathbf{s}_i^{'''}\right\|},\\ \frac{[\mu(\boldsymbol{\alpha})]_{n,i}}{\partial \tau_i} &= 1.\end{aligned} \tag{65}$$

The elements of the FIM are calculated as

$$\begin{aligned}[I(\alpha)]_{11} &= \sum_{n=1}^{N} \frac{\left(p_{n_{01}} + s_{11}^{'''}\right)^2}{\left\|\mathbf{p}_{n_0} + \mathbf{s}_1^{'''}\right\|^2},\\ [I(\alpha)]_{12} &= \sum_{n=1}^{N} \frac{\left(p_{n_{01}} + s_{11}^{'''}\right)\left(p_{n_{02}} + s_{12}^{'''}\right)}{\left\|\mathbf{p}_{n_0} + \mathbf{s}_1^{'''}\right\|^2},\\ [I(\alpha)]_{13} &= \sum_{n=1}^{N} \frac{p_{n_{01}} + s_{11}^{'''}}{\left\|\mathbf{p}_{n_0} + \mathbf{s}_1^{'''}\right\|},\\ [I(\alpha)]_{14}, ..., [I(\alpha)]_{1(3I)} &= 0,\end{aligned}$$

$$\begin{aligned}[I(\alpha)]_{21} &= [I(\alpha)]_{12}\\ [I(\alpha)]_{22} &= \sum_{n=1}^{N} \frac{\left(p_{n_{02}} + s_{12}^{'''}\right)^2}{\left\|\mathbf{p}_{n_0} + \mathbf{s}_i^{'''}\right\|^2}\\ [I(\alpha)]_{23} &= \sum_{n=1}^{N} \frac{p_{n_{02}} + s_{12}^{'''}}{\left\|\mathbf{p}_{n_0} + \mathbf{s}_1^{'''}\right\|}\\ [I(\alpha)]_{24}, ..., [I(\alpha)]_{2(3I)} &= 0,\end{aligned}$$

$$\begin{aligned}[I(\alpha)]_{31} &= [I(\alpha)]_{13}\\ [I(\alpha)]_{32} &= [I(\alpha)]_{23}\\ [I(\alpha)]_{33} &= N\\ [I(\alpha)]_{34}, ..., [I(\alpha)]_{3(3I)} &= 0,\end{aligned}$$

$$\begin{aligned}[I(\alpha)]_{41} &= [I(\alpha)]_{42} = [I(\alpha)]_{43} = 0\\ [I(\alpha)]_{44} &= \sum_{n=1}^{N} \frac{\left(p_{n_{01}} + s_{21}^{'''}\right)^2}{\left\|\mathbf{p}_{n_0} + \mathbf{s}_2^{'''}\right\|^2},\\ [I(\alpha)]_{45} &= \sum_{n=1}^{N} \frac{\left(p_{n_{01}} + s_{21}^{'''}\right)\left(p_{n_{02}} + s_{22}^{'''}\right)}{\left\|\mathbf{p}_{n_0} + \mathbf{s}_2^{'''}\right\|^2},\\ [I(\alpha)]_{46} &= \sum_{n=1}^{N} \frac{p_{n_{01}} + s_{21}^{'''}}{\left\|\mathbf{p}_{n_0} + \mathbf{s}_2^{'''}\right\|},\\ [I(\alpha)]_{47}, ..., [I(\alpha)]_{4(3I)} &= 0,\end{aligned}$$

$$\begin{aligned}[I(\alpha)]_{51} &= [I(\alpha)]_{52} = [I(\alpha)]_{53} = 0\\ [I(\alpha)]_{54} &= [I(\alpha)]_{45},\\ [I(\alpha)]_{55} &= \sum_{n=1}^{N} \frac{\left(p_{n_{01}} + s_{22}^{'''}\right)^2}{\left\|\mathbf{p}_{n_0} + \mathbf{s}_2^{'''}\right\|^2},\\ [I(\alpha)]_{56} &= \sum_{n=1}^{N} \frac{p_{n_{01}} + s_{22}^{'''}}{\left\|\mathbf{p}_{n_0} + \mathbf{s}_2^{'''}\right\|},\\ [I(\alpha)]_{57}, ..., [I(\alpha)]_{5(3I)} &= 0,\end{aligned}$$

$$\begin{aligned}[I(\alpha)]_{61}, ..., [I(\alpha)]_{63} &= 0\\ [I(\alpha)]_{64} &= [I(\alpha)]_{46}\\ [I(\alpha)]_{65} &= [I(\alpha)]_{56}\\ [I(\alpha)]_{66} &= N\\ [I(\alpha)]_{67}, ..., [I(\alpha)]_{6(3I)} &= 0\end{aligned}$$

$$\begin{aligned}[I(\alpha)]_{(3I-2)1} &= [I(\alpha)]_{(3I-2)(3I-3)} = 0\\ [I(\alpha)]_{(3I-2)(3I-2)} &= \sum_{n=1}^{N} \frac{\left(p_{n_{01}} + s_{I1}^{'''}\right)^2}{\left\|\mathbf{p}_{n_0} + \mathbf{s}_I^{'''}\right\|^2},\\ [I(\alpha)]_{(3I-2)(3I-1)} &= \sum_{n=1}^{N} \frac{\left(p_{n_{01}} + s_{I1}^{'''}\right)\left(p_{n_{02}} + s_{I2}^{'''}\right)}{\left\|\mathbf{p}_{n_0} + \mathbf{s}_I^{'''}\right\|^2},\\ [I(\alpha)]_{(3I-2)(3I)} &= \sum_{n=1}^{N} \frac{p_{n_{01}} + s_{I1}^{'''}}{\left\|\mathbf{p}_{n_0} + \mathbf{s}_I^{'''}\right\|},\end{aligned}$$

$$\begin{aligned}[I(\alpha)]_{(3I-1)1} &= [I(\alpha)]_{(3I-1)(3I-3)} = 0\\ [I(\alpha)]_{(3I-1)(3I-2)} &= [I(\alpha)]_{(3I-2)(3I-1)},\\ [I(\alpha)]_{(3I-1)(3I-1)} &= \sum_{n=1}^{N} \frac{\left(p_{n_{01}} + s_{I2}^{'''}\right)^2}{\left\|\mathbf{p}_{n_0} + \mathbf{s}_I^{'''}\right\|^2},\end{aligned}$$

$$
\begin{aligned}
[I(\alpha)]_{(3I-1)(3I)} &= \sum_{n=1}^{N} \frac{p_{n_{01}} + s_{I2}^{'''}}{\left\| \mathbf{p}_{n_0} + \mathbf{s}_I^{'''} \right\|}, \\
[I(\alpha)]_{(3I)(1)}, ..., [I(\alpha)]_{(3I)(3I-3)} &= 0. \\
[I(\alpha)]_{(3I)(3I-2)} &= [I(\alpha)]_{(3I-2)(3I)}. \\
[I(\alpha)]_{(3I)(3I-1)} &= [I(\alpha)]_{(3I-1)(3I)}. \\
[I(\alpha)]_{(3I)(3I)} &= N. \qquad (66)
\end{aligned}
$$

Similar as in Appendix A, we can build the FIM matrix using the above derivations and calculate the inverse to derive the CRLB for the parameters $\mathbf{s}_i^{'''}$ and τ_i for $i = 1, ..., I$.

Abbreviations

GNSS: Global navigation satellite systems; GLRT: Generalized likelihood ratio test; SR-LS: Squared range-least squares; CRLB: Cramér-Rao lower bound

Acknowledgements

The simulations were performed on resources provided by the Swedish National Infrastructure for Computing (SNIC) at High Performance Computing Center North (HPC2N).

Authors' contributions

Both authors have contributed to this work. Both authors read and approved the final manuscript.

Funding

This work was supported in part by Security-Link and by the SURPRISE project funded by the Swedish Foundation for Strategic Research (SSF). Open access funding provided by Linköping University.

Availability of data and materials

Not applicable.

Ethics approval and consent to participate

Not applicable.

Consent for publication

Not applicable.

Competing interests

The authors declare that they have no competing interests.

Author details

[1]Ericsson Research, Ericsson AB, Lund, Sweden. [2]Department of Electrical and Computer Engineering (ISY), Linköping University, 581 83 Linköping, Sweden.

Received: 5 September 2019 Accepted: 9 January 2020
Published online: 26 February 2020

References

1. J. V. Carroll, Vulnerability assessment of the U.S. transportation infrastructure that relies on the global positioning system. J. Navig. **56**(2), 185–193 (2003)
2. T. E. Humphreys, in *Proceedings of the Institute of Navigation GNSS (ION GNSS)*. Assessing the spoofing threat: development of a portable GPS civilian spoofer (Savannah International Convention Center, Savannah, 2008)
3. A. Cavaleri, B. Motella, M. Pini, M. Fantino, in *ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC)*. Detection of spoofed GPS signals at code and carrier tracking level, (2010)
4. K. D. Wesson, D. P. Shepard, J. A. Bhatti, T. E. Humphreys, *An evaluation of the vestigial signal defense for civil GPS anti-spoofing*, (Portland, 2011), pp. 2646–2656
5. J. M. Parro-Jimenez, R. T. Ioannides, M. Crisci, J. A. Lopez-Salcedo, in *ESA Workshop on Satellite Navigation Technologies (Navitec) and European Workshop on GNSS Signals and Signal Process*. Detection and mitigation of non-authentic GNSS signals: preliminary sensitivity analysis of receiver tracking loops, (Noordwijk, 2012)
6. M. T. Gamba, B. Motella, M. Pini, in *International Conference on Localization and GNSS (ICL-GNSS)*. Statistical test applied to detect distortions of GNSS signals, (Turin, 2013)
7. A. Broumandan, A. J. Jahromi, S. Daneshmand, G. Lachapelle, in *International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS)*. Effect of tracking parameters on GNSS receivers vulnerability to spoofing attack, (Portland, 2016), pp. 3033–3043
8. J. Huang, L. Lo Presti, B. Motella, M. Pini, GNSS spoofing detection: theoretical analysis and performance of the ratio test metric in open sky. ICT Express. **2**(1), 37–40 (2016)
9. A. Pirsiavash, A. Broumandan, G. Lachapelle, in *ESA/ESTEC NAVITEC Conference*. Two-dimensional signal quality monitoring for spoofing detection, (Noordwijk, 2016)
10. A. Broumandan, R. Siddakatte, G. Lachapelle, An approach to detect GNSS spoofing. IEEE Aerosp. Electron. Syst. Mag. **32**(8), 64–75 (2017)
11. A. Farhadi, M. Moazedi, M. R. Mosavi, A. Sadr, A novel ratio-phase metric of signal quality monitoring for real-time detection of GPS interference. Wirel. Pers. Commun. **97**(2), 2799–2818 (2017)
12. Y. Guo, L. Miao, X. Zhang, Spoofing detection and mitigation in a multi-correlator GPS receiver based on the maximum likelihood principle. **19**(37), 1–17 (Sensors 2019. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6339142/)
13. S. Semanjski, A. Muls, I. Semanjski, W. De Wilde, in *International Conference on Localization and GNSS (ICL-GNSS)*. Use and validation of supervised machine learning approach for detection of gnss signal spoofing, (nuremberg, 2019), pp. 1–6
14. A. J. Jahromi, A. Broumandan, J. Nielsen, G. Lachapelle, GPS spoofer countermeasure effectiveness based on signal strength, noise power, and C/N_0 measurements. Int. J. Satell. Commun. Netw. **30**(4), 181–191 (2012)
15. V. Dehghanian, J. Nielsen, G. Lachapelle, GNSS spoofing detection based on signal power measurements: statistical analysis. Int. J. Navig. Obs. **2012** (2012). https://www.hindawi.com/journals/ijno/2012/313527/
16. D. Yuan, H. Li, M. Lu, in *IEEE/ION Position, Location and Navigation Symposium (PLANS)*. A method for GNSS spoofing detection based on sequential probability ratio test, (Monterey, 2014), pp. 351–358
17. J. Li, J. Zhang, S. Chang, M. Zhou, Performance evaluation of multimodal detection method for GNSS intermediate spoofing. IEEE Access. **4**, 9459–9468 (2017)
18. C. Sun, J. W. Cheong, A. G. Dempster, L. Demicheli, E. Cetin, H. Zhao, W. Feng, Moving variance-based signal quality monitoring method for spoofing detection. GPS Solutions. **22**, 83 (2018)
19. W. Wang, N. Li, R. Wu, P. Closas, Detection of induced gnss spoofing using s-curve-bias. Sensors. **19**(4), 922 (2019)
20. K. D. Wesson, B. L. Evans, T. E. Humphreys, in *IEEE Global Conference on Signal and Inf. Process.* A combined symmetric difference and power monitoring GNSS anti-spoofing technique, (Austin, 2013), pp. 217–220
21. K. D. Wesson, J. N. Gross, T. E. Humphreys, B. L. Evans, GNSS signal authentication via power and distortion monitoring. IEEE Trans. Aerosp. Electron. Syst. **54**(2), 739 –754 (2017)
22. P. Y. Montgomery, T. E. Humphreys, B. M. Ledvina, in *International Technical Meeting of The Institute of Navigation*. Receiver-autonomous spoofing detection: experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer, (Savannah, 2009), pp. 124–130
23. M. Meurer, A. Konovaltsev, M. Cuntz, C. Hättich, Robust joint multi-antenna spoofing detection and attitude estimation using direction assisted multiple hypotheses RAIM. J. Inst. Navig., 3007–3016 (2012)
24. D. Borio, PANOVA tests and their application to GNSS spoofing detection. IEEE Trans. Aerosp. Electron. Syst. **49**(1), 381–394 (2013)
25. M. L. Psiaki, B. W. O'Hanlon, S. P. Powell, J. A. Bhatti, K. D. Wesson, T. E. Humphreys, A. Schofield, in *International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS)*. GNSS spoofing detection using two-antenna differential carrier phase, (Tampa, 2014)
26. A. Konovaltsev, S. Caizzone, M. Cuntz, M. Meurer, in *International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS)*. Autonomous spoofing detection and mitigation with a miniaturized adaptive antenna array, (Tampa, 2014)
27. D. Borio, C. Gioia, A sum-of-squares approach to GNSS spoofing detection. IEEE Trans. Aerosp. Electron. Syst. **52**(4), 1756–1768 (2016)

28. Y. Hu, S. Bian, B. Li, L. Zhou, A novel array-based spoofing and jamming suppression method for GNSS receiver. IEEE Sensors J. **18**(7), 2952–2958 (2018)
29. Z. Zhang, X. Zhan, Statistical analysis of spoofing detection based on tdoa. IEEJ Trans. Electr. Electron. Eng. **13**(6), 840–850 (2018). Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/tee.22637. Accessed 01 Feb 2018
30. J. Magiera, A multi-antenna scheme for early detection and mitigation of intermediate GNSS spoofing. Sensors. **19**(10), 2411 (2019)
31. Z. Gülgün, E. G. Larsson, P. Papadimitratos, in *International Symposium on Wireless Communication Systems (ISWCS), Oulu, Finland* (IEEE international conference, 2019), pp. 677–681
32. A. Broumandan, A. Jafarnia-Jahromi, V. Dehghanian, J. Nielsen, G. Lachapelle, in *IEEE/ION Position, Location and Navigation Symposium*. GNSS spoofing detection in handheld receivers based on signal spatial correlation, (Myrtle Beach, 2012), pp. 479–487
33. H. Li, X. Wang, in *IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*. Detection of GPS spoofing through signal multipath signature analysis, (Vancouver, 2016)
34. S.-H. Seo, B.-H. Lee, S.-H. Im, G.-I. Jee, K.-S. Kim, Efficient spoofing identification using baseline vector information of multiple receivers. GPS Solutions. **22**, 115 (2018)
35. M. L. Psiaki, S. P. Powell, B. W. O'Hanlon, in *Proceedings of the ION GNSS*. GNSS spoofing detection using high-frequency antenna motion and carrier-phase data, (Nashville, 2013), pp. 2949–2991
36. F. Wang, H. Li, M. Lu, GNSS spoofing countermeasure with a single rotating antenna. IEEE Access. **5**, 8039–8047 (2017)
37. P. F. Swaszek, R. J. Hartnett, in *International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+)*. Spoof detection using multiple GNSS receivers in safety critical applications, (Miami, 2013)
38. P. F. Swaszek, R. J. Hartnett, in *International Technical Meeting of The Institute of Navigation*. A multiple COTS receiver GNSS spoof detector – extensions, (San Diego, 2014)
39. E. Axell, E. G. Larsson, D. Persson, in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. GNSS spoofing detection using multiple mobile COTS receivers, (South Brisbane, 2015), pp. 3192–3196
40. E. Axell, M. Alexandersson, T. Lindgren, in *International Conference on Location and GNSS (ICL-GNSS)*. Results on GNSS meaconing detection with multiple GNSS receivers, (Gothenburg, 2015)
41. K. Jansen, N. O. Tippenhauer, C. Pöpper, in *Annual Conference on Computer Security Applications*. Multi-receiver GPS spoofing detection: Error models and realization, (New York, 2016), pp. 237–250
42. N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, S. Capkun, in *ACM Conference on Computer and Communications Security*. On the requirements for successful GPS spoofing attacks, (Chicago, 2011)
43. P. F. Swaszek, R. J. Hartnett, K. C. Seals, in *International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+)*. Using range information to detect spoofing in platoons of vehicles, (Portland, 2017), pp. 2838–2853
44. D. Radin, P. F. Swaszek, K. C. Seals, R. J. Hartnett, in *International Technical Meeting of The Institute of Navigation*. GNSS spoof detection based on pseudoranges from multiple receivers, (Tampa, 2015), pp. 657–671
45. P. F. Swaszek, R. J. Hartnett, K. C. Seals, in *International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS)*. GNSS spoof detection using passive ranging, (Portland, 2016), pp. 2971–2980
46. Z. Zhang, X. Zhan, GNSS spoofing network monitoring based on differential pseudorange. Sensors. **16**(10) (2016)
47. F. Wang, H. Li, M. Lu, GNSS spoofing detection based on unsynchronized double-antenna measurements. IEEE Access. **6**, 31203–31212 (2018)
48. A. Beck, P. Stoica, J. Li, Exact and approximate solutions of source localization problems. IEEE Trans. Sig. Process. **56**(5), 1770–1778 (2008)
49. T. E. Humphreys, in *Proceedings of the Institute of Navigation GNSS (ION GNSS)*. Assessing the spoofing threat: development of a portable GPS civilian spoofer, (Savannah, 2008)
50. J. A. García-Molina, J. A. Fernández-Rubio, in *Proceedings of the 32nd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+)*. Collaborative snapshot positioning via distributed array processing, (Miami, 2019)
    Jean-Pierre Tignol, Université Catholique de Louvain, Belgium, GaloisŠ theory of algebraic equations, World Scientific Publishing, Singapore, 2001
51. E. G. Larsson, D. Danev, Accuracy comparison of LS and squared-range LS for source localization. IEEE Trans. Sig. Process. **58**(2), 916–923 (2010)
52. S. P. Chepuri, G. Leus, A. van der Veen, Rigid body localization using sensor networks. IEEE Trans. Sig. Process. **62**(18), 4911–4924 (2014)
53. S. Chen, K. C. Ho, Accurate localization of a rigid body using multiple sensors and landmarks. IEEE Trans. Sig. Process. **63**(24), 6459–6472 (2015)
54. J. J. More, Generalizations of the trust region problem. Optim. Methods Softw. **2**(3-4), 189–209 (1993)
55. J. Tignol, *Université Catholique de Louvain, Belgium, GaloisŠ theory of algebraic equations*. (World Scientific Publishing, Singapore, 2001)
56. D. Slepian, Estimation of signal parameters in the presence of noise. Trans. IRE Prof. Group Inf. Theory. **3**(3), 68–89 (1954)

Publisher's Note