ATLANTIS PRESS

Advances in Engineering Research, volume 138

2nd International Conference on Machinery, Electronics and Control Simulation (MECS 2017)

GNSS Spoofing Interference Source Localization Using Pseudo-range and RSS Measurements

Ling Xiao [1,2,a,*], Yiming Zeng[2,b], Xushuai Li[2,c]

[1] College of Electronic Science and Engineering, National University of Defense Technology, Changsha 410073, China

[2] Xichang Satellite Launch Center, Wenchang 571300, China

[a] xiaoling_nudt@163.com, [b] yiming_4528@qq.com, [c]xusmli@mail.ustc.edu.cn

Keywords: GNSS Spoofing Interference, Pseudo-range mesurments, RSS Measurements, Source Localization.

Abstract: Global navigation satellite system (GNSS) spoofing interference can mislead the target receiver in reporting wrong position, velocity and time results, which is a serious threat to the security of GNSS applications. Localizing and destroying the interference source is a complete way to clear the threat. In this paper, an algorithm is proposed to locate interference source using both pseudo-range and received signal strength (RSS) measurements, which are from the spatially distributed GNSS receivers. The algorithm has two stages. In the first stage, the distances between the interference source and receivers are estimated using weighted least-squares (WLS) method. And then source position is estimated using the estimated distances in the second stage. This algorithm's computation burden is low, and its solution doesn't divergence even if the measurements' accuracy is low. In addition, the mathematical derivation shows that the solution can reach the CRLB accuracy. Simulations corroborate the theoretical results and the good performance of the proposed method.

1. Introduction

With the development of GNSS, it is playing a more and more important role in our daily life. As GNSS signals become very weak when they reach the earth, the signals are vulnerable to in-band interferences. Among them, the spoofing interference is the most harmful one. The structure and power of spoofing signals are very similar to the authentic ones. Its aim is to mislead the target receiver in reporting false position, velocity and time solution without being noticed by the user. It may cause serious consequences, especially for the important infrastructure using GNSS services. For example, if the timing GNSS receivers used by smart grid were spoofed, and the time solution were dragged away, it may cause power transmitting failure [1].

Therefore anti-spoofing techniques have become a hot research topic within the GNSS discipline. Researchers have proposed many anti-spoofing methods, such as: in-band power monitoring [2], signal quality monitoring [3], receiver clock monitoring [4], navigation message authentication [5], multi-antenna techniques [6], multi-receiver techniques [7] and so on. These methods are all focus on detecting and mitigating spoofing interference. However, literatures about locating spoofing source are few.

Range and received signal power are two basic measurements of GNSS receiver. Thus many existing passive source localization algorithms using TDOA measurements or energy measurements are candidates that can be used to locate spoofing source. Maximum likelihood (ML) method [8] is an attractive method, as its solution can achieve the CRLB. However, it requires iterative search and good initial guesses. And it may suffer from divergence and local convergence problem. Therefore, closed-form solutions have been proposed, such as spherical intersection [9], spherical interpolation [10], and quadratic-correction least-squares (QCLS) [11][12]. These methods perform well for the applications with high quality measurement. However, if the measurements are bad, the estimation accuracy will decline sharply.

This paper proposes a spoofing source localization algorithm using both Pseudo-range and RSS measurements from spatially distributed GNSS receivers. The receivers are static, with known positions, and using a common sampling clock to eliminate the clock bias between different receivers. The received signals are assumed direct line-of-sight and free space propagations. These assumptions have been commonly used in the previous works. The proposed method has two stages. In the first stage, the measurements functions are linearized versus the distances that between spoofing source and receivers. And the distances are estimated using WLS method. Once we obtain distances, it becomes a classical problem that resolves position from distance. The classical WLS method is used in the second stage to locate source. As the first estimator is a close-form solution and the second stage process converges quickly, the computation burden of proposed algorithm is low. In addition, the solution accuracy is analyzed. It shows that the solution can reach CRLB accuracy.

The proposed algorithm is carried out after detecting of spoofing signals. We can use the method in [7] to detect spoofing signals. This paper is focus on locating spoofing source. And the spoofing detection will not repeat more in this paper.

This paper is organized as follows: the measurements models are introduced in section 2. The localization algorithms are derived in section 3. In section 4, the localization accuracy is analyzed and compared with CRLB. Simulations are conducted in section 5. Finally, the conclusion is drawn in section 6.

2. Measurement Models

As shown in figure1, the source locating system is assumed to consist of N GNSS receivers located at positions $\mathbf{r}_i = [x_i, y_i, z_i]^T$ in Cartesian coordinates. And the spoofing source is located at $\mathbf{u}^o = [x^o, \mathrm{y}^o, \mathrm{z}^o]^T$, where $(\cdot)^o$ denotes the real value without noise.

Under the conditions of direct line-of-sight and free space propagations, the signal arriving at receiver i is [13]:

$$x_i(t) = \frac{\sqrt{p_T g_i}}{d_i^o} F(t - \tau_i) + \xi_i \tag{1}$$

Where p_T is transmitting power at the emitting source. g_i is the receiver processing gain, which can be calibrated. $d_i^o = \left\| \mathbf{u}^o - \mathbf{r}_i \right\|$ is the Euclidean distance between the source and the ith receiver. $F(t)$ is the received wave form, which is generated by modulating pseudo-random noise (PRN) codes and data message to radio frequency carriers. τ_i is the propagation delay. ξ_i is independent zero-mean Gaussian noise with variance $\sigma_{\xi_i}^2 = N_0 B$, N_0 is the noise power spectral density, and B is the signal frequency bandwidth.

We assume the spoofing source is near the ground, the spoofing signal does not travel through the ionosphere and troposphere. Therefore the ionosphere delay and troposphere delay are zeros. Therefore, the measured transmitting delay of spoofing signal includes four main components: the distance from source to receiver, the false delay τ_f simulated by the spoofer and the clock biases dt_s, dt_r of the source and receivers respectively. The pseudo-range measurement model of spoofing signal at receiver i is:

$$\rho_i = d_i^o + c\tau_f + c\left(dt_r - dt_s\right) + \varepsilon_{\rho,i} \tag{2}$$

Where c is the velocity of light. $\varepsilon_{\rho,i}$ is measurement noise, which is independent zero-mean Gaussian noise. $\sigma_{\rho,i}$ approximately equals $cT_c\sqrt{(B_L D)/(2\mathrm{CNR}_i)}$ in meters [13]. Where T_c is the

code chip duration (for GPS L1CA code, $T_c = 1/1023$ ms). B_L is the code loop filter bandwidth. CNR_i is the carrier to noise ratio, which is defined as

$$\mathrm{CNR}_i = \frac{p_T g_i}{N_0 d_i^{o2}} \tag{3}$$

As the receivers are time synchronized, the clock biases of the receivers are same. When taking difference of the pseudo- ranges, the common terms are removed. Without lose generality, choosing receiver 1 as reference, the TDOA measurement model can be represented as

$$k_{i1} = \rho_i - \rho_1 = d_i^o - d_1^o + \varepsilon_{k,i1} \tag{4}$$

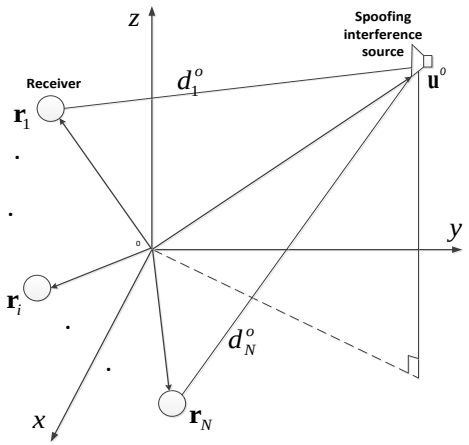

Figure 1 Spatial illustration of spoofing source localization scenario

where $\varepsilon_{k,i1} = \varepsilon_{\rho,i} - \varepsilon_{\rho,1}$. Let $\mathbf{k} = [k_{21}, k_{31}, ..., k_{N1}]^T$, it follows the joint Gaussian distribution. And its covariance matrix is $\mathbf{Q}_k$.

After dispreading and coherent integrating of the received signal, we get the received signal amplitude:

$$a_i = \frac{1}{T}\int_0^T x_i(t)F^*(t)dt = \frac{\sqrt{p_T g_i}}{d_i^o} + \xi_i' \tag{5}$$

Where T is the integrating interval. $(\cdot)^*$ denotes to take conjugation. ξ_i' is the processing result of the noise term in (1). It is also a zero-mean Gaussian random variable. And its variance is N_0/T . Let $\mathbf{a} = \left[a_1, a_2, ..., a_N\right]^T$, the covariance matrix of $\mathbf{a}$ is $\mathbf{Q}_a = diag\left\{\left[\sigma_{a,1}^2, \sigma_{a,2}^2, ..., \sigma_{a,N}^2\right]\right\} = \frac{N_0}{T}\mathbf{I}_N$. $\mathbf{I}_n$ is a n -dimension identity matrix.

3. Spoofing Source Localization

As the RSS measurements $\mathbf{a}$ contain uninteresting unknown variable p_T , the proposed solution does not use $\mathbf{a}$ directly but rather the amplitudes ratios.

Again taking receiver 1 as the reference, the amplitude ratio is:

$$q_{i1} = \frac{a_1/\sqrt{g_1}}{a_i/\sqrt{g_i}} = \frac{d_i^o}{d_1^o} \cdot \frac{1 + \varepsilon_{\mathrm{a},1} \cdot d_1^o/\sqrt{p_T g_1}}{1 + \varepsilon_{\mathrm{a},i} \cdot d_i^o/\sqrt{p_T g_i}} \tag{6}$$

When the integrating interval is sufficiently long so that the signal to noise ratio (SNR) is large enough, we have $\eta_i = (p_T g_i)/(d_i^{o2}\sigma_{a,i}^2) >> 1$. Taking Taylor expansion and ignoring the second-order and above noise terms, yields

$$q_{i1} \approx \frac{d_i^o}{d_1^o}\left(1+\frac{d_1^o \varepsilon_{\mathrm{a},1}}{\sqrt{p_T g_1}}\right)\left(1-\frac{d_i^o \varepsilon_{\mathrm{a},i}}{\sqrt{p_T g_i}}\right) \approx \frac{d_i^o}{d_1^o}+\left(\frac{d_i^o \varepsilon_{\mathrm{a},1}}{\sqrt{p_T g_1}}-\frac{d_i^{o2} \varepsilon_{\mathrm{a},i}}{d_1^o \sqrt{p_T g_i}}\right) \tag{7}$$

Collecting q_{i1} to form the vector $\mathbf{q}=[q_{21},...,q_{N1}]^T$, the covariance matrix of $\mathbf{q}$, $\mathbf{Q}_q$ has elements:

$$\mathbf{Q}_q[i-1,j-1]=\begin{cases}\dfrac{d_i^o d_j^o \sigma_{\mathrm{a},1}^2}{p_T g_1}, & i \neq j \\ \dfrac{d_i^{o2}\sigma_{\mathrm{a},1}^2}{p_T g_1}+\dfrac{d_i^{o4}\sigma_{\mathrm{a},i}^2}{d_1^{o2} p_T g_i}, & i=j\end{cases} \tag{8}$$

for $i, j = 2,3,...,N$.

We now develop the solution using (4) and (7). It has two stages. The first algorithm stage uses $\mathbf{k}$ and $\mathbf{q}$ to obtain the estimates of distances $\mathbf{d^o}=[d_1^o,...,d_N^o]^T$. And the source position is resolved in stage two of the algorithm using the estimated distances.

Stage1 Transposing the noise term to left and others to right of (4) and (7), we get the measurements error functions:

$$\Delta k_{i1} = k_{i1} - (d_i^o - d_1^o) \tag{9}$$

$$\Delta q_{i1} = q_{i1} - d_i^o / d_1^o \tag{10}$$

where $\Delta k_{i1}, \Delta q_{i1}$ denote the measurements errors of TDOA and amplitude ratio respectively.

Multiplying both side of (10) by d_1^o, yields

$$d_1^o \Delta q_{i1} = d_1^o q_{i1} - d_i^o \tag{11}$$

It can be seen that (9) and (11) are linear functions of unknown variables $\mathbf{d^o}$. Their matrix form is

$$\mathbf{e}_1 = \mathbf{h}_1 - \mathbf{G}_1 \mathbf{d}^o \tag{12}$$

$$\mathbf{e}_1 = [\Delta \mathbf{k}^T, \quad d_1^o \Delta \mathbf{q}^T]^T \tag{13}$$

$$\mathbf{h}_1 = \left[\mathbf{k}^T, \quad \mathbf{0}_{1\times N-1}\right]^T \tag{14}$$

$$\mathbf{G}_1 = \left[\mathbf{G}_{1k}^T, \quad \mathbf{G}_{1q}^T\right]^T \tag{15}$$

where $\Delta\mathbf{k}=\left[\Delta k_{21}, \Delta k_{31},..., \Delta k_{N1}\right]^T$, $\Delta\mathbf{q}=\left[\Delta q_{21}, \Delta q_{31},..., \Delta q_{N1}\right]^T$, $\mathbf{G}_{1k}=\left[-\mathbf{1}_{N-1\times 1}, \quad \mathbf{I}_{N-1}\right]$, and $\mathbf{G}_{1q}=\left[-\mathbf{q}, \quad \mathbf{I}_{N-1}\right]$. $\mathbf{0}_{1\times n}$ denotes n-dimension column vector of zeros. $\mathbf{1}_{n\times 1}$ denotes n-dimension row vector of ones.

Define the weighting matrix $\mathbf{W_1}$ as

$$\mathbf{W_1} = E[\mathbf{e_1}\mathbf{e_1^T}]^{-1} = diag\left\{\left[\mathbf{Q}_k^{-1}, \frac{1}{d_1^{o2}}\mathbf{Q}_q^{-1}\right]\right\} \tag{16}$$

Then the WLS solution to minimize $\mathbf{e}_1^T \mathbf{W_1} \mathbf{e}_1$ is [14]

$$\mathbf{d} = (\mathbf{G}_1^T \mathbf{W}_1 \mathbf{G}_1)^{-1} \mathbf{G}_1^T \mathbf{W}_1 \mathbf{h}_1 \tag{17}$$

The covariance matrix of $\mathbf{d}$ is evaluated using perturbation approach. Putting $\mathbf{h}_1 = \mathbf{h}_1^o + \Delta\mathbf{h}_1$ and $\mathbf{G}_1 = \mathbf{G}_1^o + \Delta\mathbf{G}_1$ in (12), and noting $\mathbf{h}_1^o = \mathbf{G}_1^o\mathbf{d}^o$, we get:

$$\mathbf{e}_1 = \Delta\mathbf{h}_1 - \Delta\mathbf{G}_1\mathbf{d}^o \tag{18}$$

Let $\mathbf{d} = \mathbf{d}^o + \Delta\mathbf{d}$, multiplying both sides of (17) by $(\mathbf{G}_1^T\mathbf{W}_1\mathbf{G}_1)$, we arrive:

$$\begin{aligned}&(\mathbf{G}_1^o + \Delta\mathbf{G}_1)^T\,\mathrm{W}_1(\mathbf{G}_1^o + \Delta\mathbf{G}_1)(\mathbf{d}^o + \Delta\mathbf{d})\\ &= (\mathbf{G}_1^o + \Delta\mathbf{G}_1)^T\,\mathrm{W}_1(\mathbf{h}_1^o + \Delta\mathbf{h}_1)\end{aligned} \tag{19}$$

Ignoring the second and higher order perturbation terms, and using (18), the $\Delta\mathbf{d}$ and its covariance matrix are:

$$\begin{aligned}\Delta\mathbf{d} &= (\mathrm{G}_1^{oT}\mathrm{W}_1\mathrm{G}_1^o)^{-1}\,\mathrm{G}_1^{oT}\mathrm{W}_1\,\mathbf{e}_1\\ \mathrm{cov}(\mathbf{d}) &= (\mathrm{G}_1^{oT}\mathrm{W}_1\mathrm{G}_1^o)^{-1}\end{aligned} \tag{20}$$

Stage 2 The classical iterative WLS method is used to estimate source position using the estimated distances from stage 1. By given an initial guess $\mathbf{u}_g$, the resolving procedure is

$$\begin{aligned}&i = 0, \mathbf{u}^{(0)} = \mathbf{u}_g\\ &\left[\begin{array}{l} \textit{while} \quad \left\|\Delta\mathbf{u}^{(i)}\right\| > \mu\\ \Delta\mathbf{u}^{(i+1)} = (\mathbf{G}_2^{(i)T}\mathbf{W}_2\mathbf{G}_2^{(i)})^{-1}\mathbf{G}_2^{(i)T}\mathbf{W}_2\Delta\mathbf{d}^{(i)}\\ \mathbf{u}^{(i+1)} = \mathbf{u}^{(i)} + \Delta\mathbf{u}^{(i+1)}\\ i = i+1\end{array}\right.\end{aligned} \tag{21}$$

where

$$\Delta\mathbf{u} = [\Delta x, \Delta y, \Delta z]^T \tag{22}$$

$$\mathbf{G}_2^{(i)} = \left[\frac{(\mathbf{u}^{(i)} - \mathbf{r}_1)}{\left\|\mathbf{u}^{(i)} - \mathbf{r}_1\right\|}, \ldots, \frac{(\mathbf{u}^{(i)} - \mathbf{r}_N)}{\left\|\mathbf{u}^{(i)} - \mathbf{r}_N\right\|}\right]^T \tag{23}$$

$$\Delta\mathbf{d}^{(i)} = \left[d_1 - \left\|\mathbf{u}^{(i)} - \mathbf{r}_1\right\|, \ldots, d_N - \left\|\mathbf{u}^{(i)} - \mathbf{r}_N\right\|\right]^T \tag{24}$$

$$\mathbf{W}_2 = \left(\mathrm{cov}(\mathbf{d})\right)^{-1} = \mathbf{G}_1^{oT}\mathbf{W}_1\mathbf{G}_1^o \tag{25}$$

and μ is the threshold.

When the solution $\mathbf{u}^{(i)}$ approaches $\mathbf{u}^o$, the estimation noise $\Delta\mathbf{u}$ is:

$$\Delta\mathbf{u} = (\mathbf{G}_2^{oT}\mathbf{W}_2\mathbf{G}_2^o)^{-1}\mathbf{G}_2^{oT}\mathbf{W}_2\Delta\mathbf{d} \tag{26}$$

Therefore the covariance matrix of the solution is:

$$\mathrm{cov}(\mathbf{u}) = \left[\left(\mathbf{G}_1^o\mathbf{G}_2^o\right)^T\,\mathbf{W}_1\left(\mathbf{G}_1^o\mathbf{G}_2^o\right)\right]^{-1} \tag{27}$$

To summarize, the proposed solution consists of (17) and (21). The weighting matrix $\mathbf{W}_1$ is given in (16). Note that the weighting matrix $\mathbf{W}_1$ involves the true source position because $\mathbf{Q}_q$ in (8) depends on d_i^o, $i = 1, 2, \ldots, N$ and p_T. For implementation purpose, we shall first set $\mathbf{W}_1$ to identity and use (17) to obtain an initial estimate of $\mathbf{d}$. We then apply this initial estimate to form $\mathbf{W}_1$ and use this approximated $\mathbf{W}_1$ to find a better $\mathbf{d}$. In the second stage, an initial guess $\mathbf{u}_g$ should be given. We choose the first stage rough solution of Ho's algorithm [11] as the starting point of the iteration.

4. CRLB and Source Localization Accuracy

In this section, the CRLB of the source localization problem is derived. And the accuracy of the proposed source localization solution is analyzed.

4.1. CRLB

According to the TDOA and RSS measurement models (4) and (5), as the processing gain g_i can be determined by calibration, the unknown parameter vector is. $\boldsymbol{\theta} = \left[\mathbf{u}^{oT}, p_T\right]^T$ g_i When the signal is tracked perfectly, it can be verified that the TDOA measurements $\mathbf{k}$ and received signal amplitude measurements **a** are independent of each other, so the logarithm of the probability density function of the measurement vector $\mathbf{m} = \left[\mathbf{k}^T, \mathbf{a}^T\right]^T$ is

$$\begin{aligned} \ln f(\mathbf{m};\boldsymbol{\theta}) = c - \frac{1}{2}\left(\mathbf{k}-\mathbf{k}^o\right)^T \mathbf{Q}_k^{-1}\left(\mathbf{k}-\mathbf{k}^o\right) \\ -\frac{1}{2}\left(\mathbf{a}-\mathbf{a}^o\right)^T \mathbf{Q}_a^{-1}\left(\mathbf{a}-\mathbf{a}^o\right) \end{aligned} \tag{28}$$

where $c = -\frac{1}{2}\ln\left((2\pi)^{2N-1}\left|\mathbf{Q}_k\right|\left|\mathbf{Q}_a\right|\right)$ is a constant. So the CRLB of $\boldsymbol{\theta}$ is :

$$\mathrm{CRLB}\left(\boldsymbol{\theta}\right) = -E\left[\frac{\partial^2 \ln f(\mathbf{m};\boldsymbol{\theta})}{\partial\boldsymbol{\theta}\partial\boldsymbol{\theta}^T}\right]^{-1} = \begin{bmatrix} \mathbf{J}_{11} & \mathbf{J}_{12} \\ \mathbf{J}_{12}^T & J_{22} \end{bmatrix}^{-1} \tag{29}$$

where

$$\begin{aligned} \mathbf{J}_{11} &= -E\left[\frac{\partial^2 \ln f(\mathbf{m};\boldsymbol{\theta})}{\partial\mathbf{u}^o\partial\mathbf{u}^{oT}}\right] = \mathbf{J}_{11t} + \mathbf{J}_{11a} \\ \mathbf{J}_{11t} &= \left(\frac{\partial\mathbf{k}^o}{\partial\mathbf{u}^o}\right)^T \mathbf{Q}_k^{-1}\left(\frac{\partial\mathbf{k}^o}{\partial\mathbf{u}^o}\right) = \mathbf{G}_{td}^{oT}\mathbf{Q}_k^{-1}\mathbf{G}_{td}^o \\ \mathbf{J}_{11a} &= \left(\frac{\partial\mathbf{a}^o}{\partial\mathbf{u}^o}\right)^T \mathbf{Q}_a^{-1}\left(\frac{\partial\mathbf{a}^o}{\partial\mathbf{u}^o}\right) = \sum_{i=1}^{N}\frac{\eta_i}{d_i^{o4}}\left(\mathbf{u}^o-\mathbf{r}_i\right)\left(\mathbf{u}^o-\mathbf{r}_i\right)^T \end{aligned} \tag{30}$$

$$\frac{\partial\mathbf{k}^o}{\partial\mathbf{u}^o} = \mathbf{G}_{td}^o = \begin{bmatrix} \frac{(\mathbf{u}^o-\mathbf{r}_2)^T}{\left\|\mathbf{u}^o-\mathbf{r}_2\right\|} - \frac{(\mathbf{u}^o-\mathbf{r}_1)^T}{\left\|\mathbf{u}^o-\mathbf{r}_1\right\|} \\ \vdots \\ \frac{(\mathbf{u}^o-\mathbf{r}_N)^T}{\left\|\mathbf{u}^o-\mathbf{r}_N\right\|} - \frac{(\mathbf{u}^o-\mathbf{r}_1)^T}{\left\|\mathbf{u}^o-\mathbf{r}_1\right\|} \end{bmatrix} \tag{31}$$

$$\begin{aligned} \mathbf{J}_{12} &= -E\left[\frac{\partial^2 \ln f(\mathbf{m};\boldsymbol{\theta})}{\partial\mathbf{u}^o\partial p_T}\right] = \left(\frac{\partial\mathbf{a}^o}{\partial\mathbf{u}^o}\right)^T \mathbf{Q}_a^{-1}\left(\frac{\partial\mathbf{a}^o}{\partial p_T}\right) \\ &= -\frac{1}{2p_T}\sum_{i=1}^{N}\frac{\eta_i}{d_i^{o2}}\left(\mathbf{u}^o-\mathbf{r}_i\right) \end{aligned} \tag{32}$$

$$\begin{aligned} J_{22} &= -E\left[\frac{\partial^2 \ln f(\mathbf{m};\boldsymbol{\theta})}{\partial p_T\partial p_T}\right] = \left(\frac{\partial\mathbf{a}^o}{\partial p_T}\right)^T \mathbf{Q}_a^{-1}\left(\frac{\partial\mathbf{a}^o}{\partial p_T}\right) \\ &= \frac{1}{4p_T^2}\sum_{i=1}^{N}\eta_i \end{aligned} \tag{33}$$

Using the block matrix inverse lemma [14], we get

$$\mathrm{CRLB}\left(\mathbf{u}^o\right)=\left(\mathbf{J}_{11}-\frac{\mathbf{J}_{12}\mathbf{J}_{12}^T}{J_{22}}\right)^{-1} \tag{34}$$

4.2. Source Location Accuracy

Putting in the relevant matrices defined in (15), (16) and (23), (27) can be recast as:

$$\begin{aligned}\mathrm{cov}(\mathbf{u})&=\left[\mathbf{M}_t+\mathbf{M}_q\right]^{-1}\\ \mathbf{M}_t&=\left(\mathbf{G}_{1t}\mathbf{G}_2^o\right)^T\mathbf{Q}_k^{-1}\left(\mathbf{G}_{1t}\mathbf{G}_2^o\right)\\ \mathbf{M}_q&=\left(\frac{1}{d_1^o}\mathbf{G}_{1q}^o\mathbf{G}_2^o\right)^T\mathbf{Q}_q^{-1}\left(\frac{1}{d_1^o}\mathbf{G}_{1q}^o\mathbf{G}_2^o\right)\end{aligned} \tag{35}$$

It can be verified that $\mathbf{G}_{1t}\mathbf{G}_2^o=\mathbf{G}_{td}^o$, thus:

$$\mathbf{M}_t=\mathbf{J}_{11t}=\mathbf{G}_{td}^{oT}\mathbf{Q}_k^{-1}\mathbf{G}_{td}^o \tag{36}$$

Let $\mathbf{D}=\left(\mathbf{G}_{1q}^o\mathbf{G}_2^o\right)\Big/d_1^o$, using the fact that $q_{i1}^o=d_i^o\Big/d_1^o$, $\mathbf{D}$ can be simplified to a matrix whose $(i-1)$th row is

$$\begin{aligned}&\mathbf{D}[i-1,:]=\frac{1}{d_1^o d_i^o}\left[\left(\mathbf{u}^o-\mathbf{r}_i^o\right)^T-\frac{d_i^{o2}}{d_1^{o2}}\left(\mathbf{u}^o-\mathbf{r}_1^o\right)^T\right]\\ &i=2,...,N\end{aligned} \tag{37}$$

The matrix $\mathbf{Q}_q$ is given in (8), it can be expressed in matrix form as

$$\mathbf{Q}_q=\mathbf{P}+\mathbf{n}\mathbf{n}^T \tag{38}$$

$$\mathbf{P}=diag\left\{\left[\frac{d_2^{o2}}{d_1^{o2}\eta_2},\frac{d_3^{o2}}{d_1^{o2}\eta_3},...,\frac{d_N^{o2}}{d_1^{o2}\eta_N}\right]\right\} \tag{39}$$

$$\mathbf{n}=\frac{1}{\sqrt{\eta_1}}\left[\frac{d_2^o}{d_1^o},\frac{d_3^o}{d_1^o},...,\frac{d_N^o}{d_1^o}\right]^T \tag{40}$$

Invoking the matrix inverse lemma [14] gives

$$\mathbf{Q}_q^{-1}=\mathbf{P}^{-1}-K\mathbf{P}^{-1}\mathbf{n}\mathbf{n}^T\mathbf{P}^{-1} \tag{41}$$

where $K=1\Big/\left(1+\mathbf{n}^T\mathbf{P}^{-1}\mathbf{n}\right)=\eta_1\Big/\sum_{i=1}^{N}\eta_i$. As a result

$$\mathbf{M}_q=\mathbf{D}^T\mathbf{Q}_q^{-1}\mathbf{D}=\mathbf{D}^T\mathbf{P}^{-1}\mathbf{D}-K\mathbf{D}^T\mathbf{P}^{-1}\mathbf{n}\mathbf{n}^T\mathbf{P}^{-1}\mathbf{D} \tag{42}$$

The first term $\mathbf{D}^T\mathbf{P}^{-1}\mathbf{D}$ is, after substituting (37) and (39)

$$\begin{aligned}\mathbf{D}^T\mathbf{P}^{-1}\mathbf{D}=\sum_{i=1}^{N}\Bigg\{&\frac{\eta_i}{d_i^{o2}}\left[\left(\mathbf{u}^o-\mathbf{r}_i^o\right)-\frac{d_i^{o2}}{d_1^{o2}}\left(\mathbf{u}^o-\mathbf{r}_1^o\right)\right]\\ &\times\left[\left(\mathbf{u}^o-\mathbf{r}_i^o\right)^T-\frac{d_i^{o2}}{d_1^{o2}}\left(\mathbf{u}^o-\mathbf{r}_1^o\right)^T\right]\Bigg\}\end{aligned} \tag{43}$$

Also, putting (37), (39) and (40) yields

$$\mathbf{D}^T\mathbf{P}^{-1}\mathbf{n}=\frac{1}{\sqrt{\eta_1}}\sum_{i=1}^{N}\frac{\eta_i}{d_i^{o2}}\left[\left(\mathbf{u}^o-\mathbf{r}_i^o\right)-\frac{d_i^{o2}}{d_1^{o2}}\left(\mathbf{u}^o-\mathbf{r}_1^o\right)\right] \tag{44}$$

Now, substituting (43), (44) and K into (42), after some straightforward simplification, we arrive at

$$\begin{aligned}\mathbf{M}_q &= \sum_{i=1}^{N}\frac{\eta_i}{d_i^{o4}}\left(\mathbf{u}^o-\mathbf{r}_i\right)\left(\mathbf{u}^o-\mathbf{r}_i\right)^T \\ &\quad -\frac{1}{\sum_{i=1}^{N}\eta_i}\sum_{i=1}^{N}\sum_{j=1}^{N}\frac{\eta_i\eta_j}{d_i^{o2}d_j^{o2}}\left(\mathbf{u}^o-\mathbf{r}_i\right)\left(\mathbf{u}^o-\mathbf{r}_j\right)^T \\ &= \mathbf{J}_{11q}-\frac{\mathbf{J}_{12}\mathbf{J}_{12}^T}{J_{22}}\end{aligned} \tag{45}$$

Substituting (36) and (45) into (35), we get

$$\mathrm{cov}(\mathbf{u}) = \left(\mathbf{J}_{11}-\frac{\mathbf{J}_{12}\mathbf{J}_{12}^T}{J_{22}}\right)^{-1} \tag{46}$$

It is identical to the CRLB as shown in (34).

Table 1 Receiver position in the unit of meter

receiver no.	1	2	3	4	5	6
x_i	0	50	-50	0	0	0
y_i	0	0	0	-50	0	0
z_i	0	0	0	0	50	-50

5. Simulations

In this section we assess the performances of the devised algorithms using Monte Carlo simulations. The number of Monte Carlo runs was 10000 times. The localization system consists of 6 receivers. Their positions are listed in TABLE I. The spoofing interference source is located at (70m, -122m, 141m), denoted as location A, (141m, 245m, 282m), denoted as location B, in the reference coordinates.

We suppose the spoofed signal was GPS L1CA signal in the simulations. The RSS measurements were generated according to the model (5). The receiver processing gains g_i were all unity. The thermal noise power spectral density $N_0 = -204\text{dB-Hz}$ .The transmitting power $p_T = 10^{(N_0/10)}\cdot \mathrm{CNR}_1 \cdot d_1^{o2}$. $\varepsilon_{a,i}$ were independent identical distributed (IID) zero-mean Gaussian random variable with variances $\sigma_{a,i}^2 = N_0/T$. The integrating interval T was 0.02s, which is the navigation data bit period of GPS L1CA signals. The spoofed range measurements were generated according to the model (2). The components τ_f , dt_r , and dt_{SI} were all zero, as they will be removed when taking difference. $\varepsilon_{\rho,i}$ were IID zero-mean Gaussian random variables. And $\sigma_{\rho,i} = cT_c\sqrt{(B_L D)/(2\mathrm{CNR}_i)}$, where $B_L = 1\text{Hz}$ and $D = 1\text{chip}$.

The simulation results of near-field source located at A are depicted in figure 2. It compares the performance of the proposed algorithm with Ho's [11] in mean-square-error (MSE), which is defined as

$$\mathrm{MSE}(\mathbf{u}) = \frac{1}{N_{sim}}\sum_{i=1}^{N_{sim}}\left\|\hat{\mathbf{u}}_i-\mathbf{u}^o\right\|^2 \tag{47}$$

where N_{sim} denotes the number of Monte Carlo runs. $\hat{\mathbf{u}}_i$ denotes the estimated position of the i-th trial. The reason, why we choose Ho's solution for comparison, is that it performs better than others provided in [9] and [10]. It can be seen that the accuracy of estimated position is improved by about 5dB for additionally using the RSS measurements. When the received signal is strong, both the

proposed solution and Ho's can achieve their CRLB accuracies respectively. When the received signal is weak, both the solutions deviate from their CRLB accuracies, but the proposed algorithm performs more robust than Ho's.

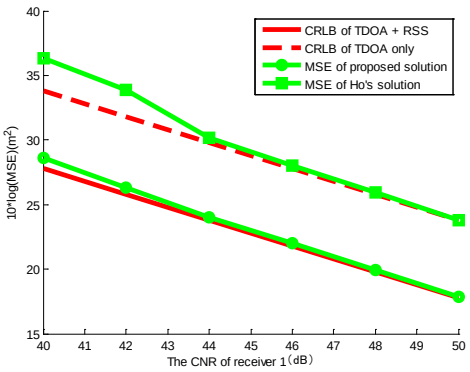

Figure 2 The position estimation performance versus different CNRs, when the source was located at A.

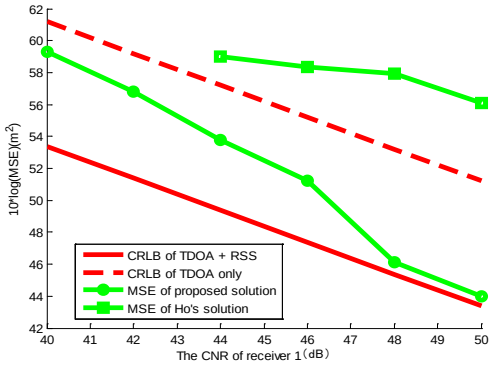

Figure 3 The position estimation performance versus different CNRs, when the source was located at B.

Figure 3 plots the results of far-field case, which the spoofing source was located at B. Also, the MSE and CRLB of the proposed solution and Ho's were given for comparison. Due to the worsening of geometry relationship between the source and receivers, the CRLB of far-field case reduces 10dB compared with near-field one. And with the decreasing of received CNR, both the solutions are deviating from their CRLB accuracies, which is even worse than the near-field case. However, the proposed solution is more robust than Ho's, as Ho's algorithm can't give an available solution when the received signal is weak.

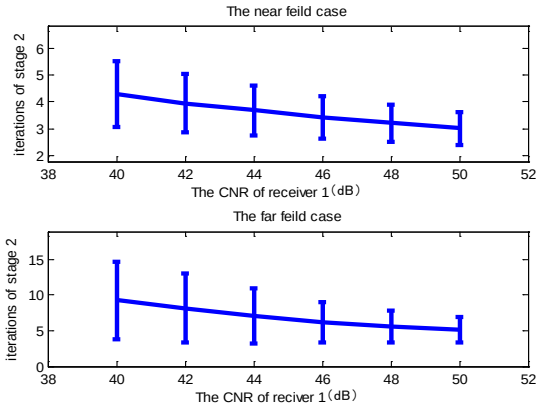

Figure 4 Convergence speeds for the second stage of proposed algorithm when the source was located at A and B.

Figure 4 depicts the mean and standard deviation of the number of iterations required in the second stage of the proposed algorithm. As shown, the convergence speed depends both on the CNR level as well as on the geometry relationship.

6. Conclusion

A GNSS spoofing interference source localization method is proposed in the paper. The proposed method locates spoofing source using TDOA and RSS measurements, under the assumptions that direct line-of-sight and free space propagation. The estimation accuracy of the proposed method is analyzed. It shows that the proposed solution can achieve CRLB accuracy when SNR is large enough. The theoretic analysis is confirmed by simulation results. In addition, the simulation results illustrate that the proposed method improves the solution accuracy for additionally using RSS measurements and performs more robust than Ho's. However the assumptions that direct line-of-sight and free space propagation may not valid in practical applications. The future work is to extend the proposed algorithm to a more realistic signal model and scenario.

References

[1] Z.Zhang, S. Gong,A.D. Dimitrovski, H. Li, “Time synchronization attack in smart grid:impact and analysis”, IEEE Transactions on Smart Grid, vol.4, no.1, pp. 87--98, 2013.

[2] Ali Jafarnia-Jahromi, Ali Broumandan, J. Nielsen and G. Lachapelle, “Pre-despreading authenticity verification for gps l1 c/a signals”, Navigation, vol.61, no.1, pp. 1--11, 2014.

[3] Heidi Kuusniemi, Mohammad Zahidul H Bhuiyan and T.Kroger, “Signal quality indicators and reliability testing for spoof-resistant gnss receivers”, European Journal of Navigation, vol.11, no.2, pp. 12--19, 2013.

[4] Ali Jafarnia-Jahromi, S.Daneshmand, Ali Broumandan, J.Nielsen and G.Lachapelle, “Pvt solution authentication based on monitoring the clock state for a moving gnss receiver”, in European Navigation Conference (ENC2013), Vienna, Austria, April 2013.

[5] T.E. Humphreys, “Detection strategy for cryptographic gnss anti-spoofing”, IEEE Transactions on Aerospace and Electronic Systems, vol.49, no.2, pp.1073--1090, 2013.

[6] M.L. Psiaki,B. W. OHanlon, S. P.Powell, et.al., “Gnss spoofing detection using two-antenna differential carrier phase”, in The 27th International Technical Meeting of The Satellite Division of the Institute of Navigation, Tampa, Florida, Sep. 2014.

[7] P.F. Swaszek and R.J. Hartnett, “Spoof detection using multiple cots receivers in safety critical applications”, in Proc. ION GNSS+2013, Nashville TN,USA, Sep. 2013.

[8] X. Sheng and Y.H. Hu, “Maximum likelihood multiple-source localization using acoustic energy measurements with wireless sensor networks”, IEEE Transactions on Signal Process, vol.53, no.1, pp. 44--53, 2005.

[9] H.C. Schau and A.Z. Robinson, “Passive source localization employing intersecting spherical surfaces from time-of-arrival differences”, IEEE Trans. Acoust., Speech, Signal Processing, vol. ASSP-35, pp.1223–1225, Aug. 1987.

[10] J.O. Smith and J.S. Abel, “Closed-form least-squares source location estimation from range-difference measurements”, IEEE Trans. Acoust.,Speech, Signal Processing, vol. ASSP-35, pp. 1661–1669, Dec. 1987.

[11] Y.T. Chm and K.C. Ho, “A simple and efficient estimator for hyperbolic location”, IEEE Transactions on Signal Processing, vol.42, no.8, pp. 1905--1915, 1994.

[12] K.C. Ho and M. Sun, “An accurate algebraic closed form solution for energy based source ocalization”, IEEE Transactions on Audio, Speech, Language Processing, vol.15, no.11, pp. 2542--2550, 2007.

[13] E.D. Kaplan and C.J. Hegarty, Understanding GPS: principles and applications. Artech House, 2nd edn. 2006.

[14] X. Zhang, Matrix Analysis and Applicaitons. Beijing,China: Tsinghua university press, 2004.(in chinese)