Chapter 56
Research of a Low Complexity Spoofing Mitigation Method Based on a Moving Antenna

Long Huang, Junwei Nie, Rui Ge and Feixue Wang

Abstract Spoofing to GNSS receivers becomes to a majority threat to satellite navigations systems in civil safety critical applications. By weighing the groups of samples from a single moving antenna precisely, an equivalent adaptive beam forming antenna array is synthesized. Corresponding to the scenario that all spoofing pseudo random noise (PRN) codes are transmitted from the same source in space, the different spatial signatures of spoofing and authentic signals are analyzed. With a low complexity weighing parameters calculations algorithm, a null is steered in the direction where spoofing signals come from. This is an effective spoofing mitigation method which greatly suppresses the energy of spoofing signals in the conventional GNSS receiver procedures. And simulation results are given in the end to the valid the performance of the proposed method.

Keywords GNSS · Satellite navigation receiver · Spoofing interference · Spoofing mitigation

56.1 Introduction

Spoofing to civil GNSS receiver aim to mislead the target receiver to a false position/timing solution, which becomes to a major threaten to the satellite navigation systems [1]. Plenty of anti-spoofing techniques have been proposed in the open literature recently. These methods can be generally divided into two main categories, namely spoofing detection and spoofing mitigation.

Spoofing detection techniques refer to discriminate the spoofing signals from the authentic ones, and exclude them off the position/timing calculation. The widely

L. Huang (✉) · J. Nie · R. Ge · F. Wang
Satellite Navigation R&D Center, National University of Defense Technology,
Changsha, China
e-mail: huangl386@hotmail.com

J. Sun et al. (eds.), *China Satellite Navigation Conference (CSNC) 2013 Proceedings*, Lecture Notes in Electrical Engineering 243,
DOI: 10.1007/978-3-642-37398-5_56, © Springer-Verlag Berlin Heidelberg 2013

discussed signal power discrimination, time of arrival (TOA) discrimination, polarization discrimination, angle of arrival (AOA) discrimination, cross-check of IMU and cryptographic authentication are all belong to this category [2–6].

Spoofing mitigation techniques refer to remove the spoofing signals in front of conventional GNSS receiver acquisition and tracking processing, which can eliminate the impact of spoofing to receiver radically. Dr. Daneshmand [7] in university of Calgary proposed a spoofing mitigation technique using multiple antennas and proved to be effective to remove spoofing signals coming from a point transmitting source. Multiple antennas technique is one of the most powerful techniques that have been devised against spoofing threat, but it increase the size and cost of GNSS receivers, which restricts the use of multiple antennas in civil domain.

In this paper, a new equivalent adaptive beam forming antenna array technique is proposed to migration spoofing signals coming from a point transmitting source. By weighing the groups of samples from a single moving antenna precisely, an equivalent adaptive beam forming antenna array is synthesized. Corresponding to the scenario that all spoofing pseudo random noise (PRN) codes are transmitted from the same source in space, the different spatial signatures of spoofing and authentic signals are analyzed. With a low complexity weighing parameters calculations algorithm, a null is steered in the direction where spoofing signals come from. This is an effective spoofing mitigation method which greatly suppresses the energy of spoofing signals in the conventional GNSS receiver procedures.

56.2 System Model

56.2.1 Receiver Signal Model

In this paper, it is assumed that the spoofer transmitting several PRN codes through a single antenna, each of which having a comparable power level to that of the authentic signals. And the spoofing and authentic signals all use periodicity PRN codes in their structures. A typical spoofing scenario is shown in Fig. 56.1.

The baseband samples of authentic and spoofing signals in GNSS receivers can be written as:

$$r(n) = \sum_{m=1}^{N_A} a_{mn}\sqrt{P_m^a}F_m^a(n) + \sum_{k=1}^{N_S} b_{kn}\sqrt{P_k^s}F_k^s(n) + \omega(nT_s) \tag{56.1}$$

where N_A and N_S are the number of authentic and spoofing PRNs respectively and

$$\begin{aligned} F_m^a(n) &= d_m^a\left(nT_s - \tau_m^a\right)c_m^a\left(nT_s - \tau_m^a\right)e^{j\phi_m^a + j2\pi f_m^a nT_s} \\ F_k^s(n) &= d_k^s\left(nT_s - \tau_k^s\right)c_k^s\left(nT_s - \tau_k^s\right)e^{j\phi_k^s + j2\pi f_k^s nT_s} \end{aligned} \tag{56.2}$$

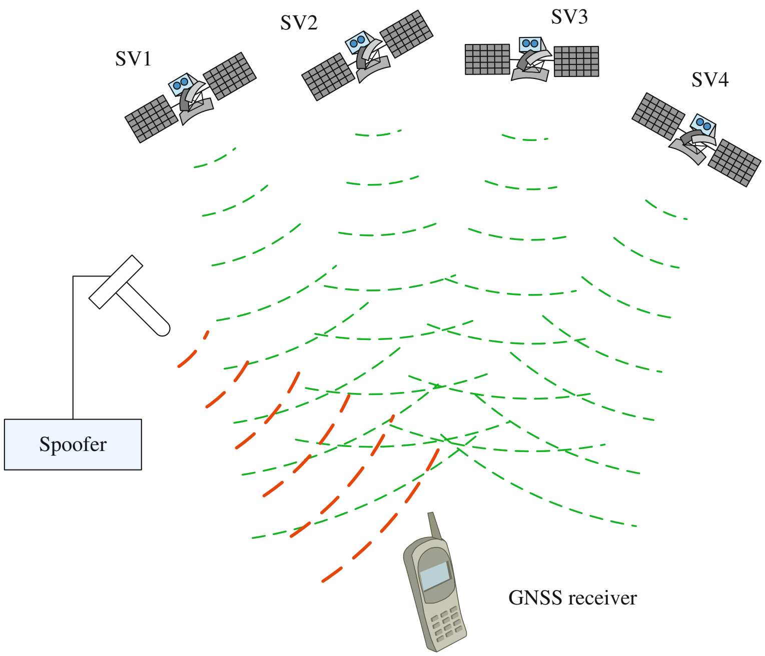


Fig. 56.1 A typical spoofing scenario

In (56.1) and (56.2), the superscripts a and s refer to the authentic and spoofing signals respectively. T_s is the sampling interval and ϕ, f, P and τ are the phase, Doppler frequency, signal power and code delay of the received signals respectively. Symbols a_{mn} and b_{kn} present the spatial attenuation-delay characteristic of the authentic and spoofing signals, while ω is the additive white Gaussian noise with variance σ^2.

56.2.2 Spoofing Mitigation Model

For a moving GNSS receiver, taking N samples out of the input sequence in (56.1) can form an equivalent N-element array antenna output vector:

$$\mathbf{R_N}(n) = \left[r(n)\ r(n-\Delta)\ r(n-\Delta)\ \ldots\ r(n-(N-1)\Delta)^T\right] \tag{56.3}$$

Without loss of generality assuming that the reference coordinate system is located at the receiver antenna at the time of r(n), as shown in Fig. 56.2.

where $\hat{\mathbf{d}}_m^A$ and $\hat{\mathbf{d}}^S$ are unit vectors pointing from the origin of the coordinate system towards the mth GNSS satellite and the spoofer respectively. $\mathbf{d}_{i1}^{ant}$ is the vector

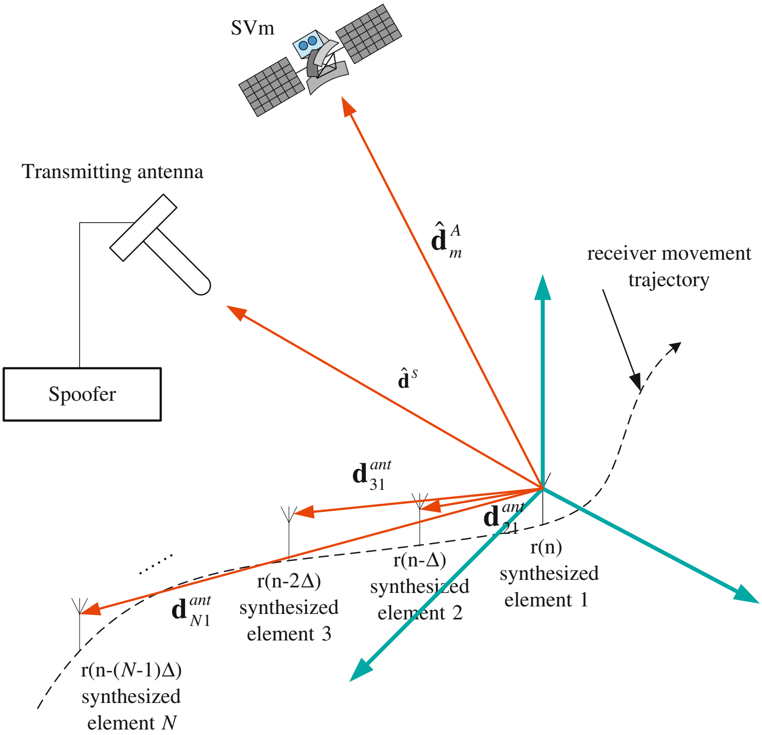


Fig. 56.2 Equivalent N-element antenna configuration

pointing from the origin to the *i*th equivalent antenna element phase center and λ is the GNSS carrier wavelength.

Taking Eqs. (56.1) and (56.2) into Eq. (56.3), the equivalent array antenna output vector can be written as:

$$\mathbf{R_N}(n) = \sum_{m=1}^{N_A} \mathbf{a_m}\sqrt{P_m^a}F_m^a(n) + \mathbf{b}\sum_{k=1}^{N_s}\sqrt{P_k^s}F_k^s(n) + \boldsymbol{\eta}(n) \tag{56.4}$$

where η is the complex additive white Gaussian noise vector with covariance matrix $\sigma^2\mathbf{I}$. $\mathbf{b}$ and $\mathbf{a_m}$ are spatial characteristic vector (SCV) of spoofing PRNs and *m*th authentic signal respectively:

$$
\begin{gathered}
\mathbf{a_m} = \mathbf{C}\overline{\mathbf{a}}_\mathbf{m} \\
\mathbf{b} = \mathbf{C}\overline{\mathbf{b}} \\
\mathbf{C} = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & C_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & C_N \end{bmatrix} \quad \overline{\mathbf{a}}_\mathbf{m} = \begin{bmatrix} 1 \\ a_{m2} \\ \vdots \\ a_{mN} \end{bmatrix} = \begin{bmatrix} 1 \\ e^{-j\frac{2\pi \mathbf{d}_{21}^{ant} \bullet \hat{\mathbf{d}}_m^A}{\lambda}} \\ \vdots \\ e^{-j\frac{2\pi \mathbf{d}_{N1}^{ant} \bullet \hat{\mathbf{d}}_m^A}{\lambda}} \end{bmatrix} \quad \overline{\mathbf{b}} = \begin{bmatrix} 1 \\ b_2 \\ \vdots \\ b_N \end{bmatrix} = \begin{bmatrix} 1 \\ e^{-j\frac{2\pi \mathbf{d}_{21}^{ant} \bullet \hat{\mathbf{d}}^S}{\lambda}} \\ \vdots \\ e^{-j\frac{2\pi \mathbf{d}_{N1}^{ant} \bullet \hat{\mathbf{d}}^S}{\lambda}} \end{bmatrix}
\end{gathered}
\tag{56.5}
$$

Consequently, the problem of spoofing mitigation with a synthesized antenna array is to find an optimal gain vector which is denoted by **f** to satisfy the following conditions:

$$
\mathbf{f}^H \mathbf{b} = 0 \text{且} \|\mathbf{f}\| \neq 0 \tag{56.6}
$$

By applying the vector **f** to the synthesized antenna array signals, the spoofing signal is suppressed in the beam former output as:

$$
\begin{aligned}
v(n) &= \mathbf{f}^H \mathbf{R_N}(n) \\
&= \sum_{m=1}^{N_A} \mathbf{f}^H \mathbf{a_m} \sqrt{P_m^a} F_m^a(n) + \mathbf{f}^H \mathbf{b} \sum_{k=1}^{N_S} \sqrt{P_k^s} F_k^s(n) + \mathbf{f}^H \boldsymbol{\eta}(n) \\
&= \sum_{m=1}^{N_A} \mathbf{f}^H \mathbf{a_m} \sqrt{P_m^a} F_m^a(n) + \mathbf{f}^H \boldsymbol{\eta}(n)
\end{aligned}
\tag{56.7}
$$

56.3 Spoofing Mitigation

The proposed spoofing mitigation technique based on a moving single antenna receiver consists of two main modules, namely spoofing SCV estimation and null steering, which are described in the following subsections.

56.3.1 Spoofing SCV Estimation

As mentioned above, the key problem of the proposed method is to find a non-zero orthogonal vector of spoofing SCV, so it's necessary to estimate the spoofing SCV at the beginning.

In order to avoid the computational complexity of the conventional two-dimensional time and frequency search for the authentic and spoofing signals, a approximate despreading processing is conducted by multiplying samples with space of Δ and one period of the PRN code.

Assume vector $\mathbf{y}$ is constructed as:

$$\mathbf{y} = \begin{bmatrix} \beta_1 e^{j\theta_1} \\ \beta_2 e^{j\theta_2} \\ \vdots \\ \beta_N e^{j\theta_N} \end{bmatrix} \tag{56.8}$$

where

$$\theta_i = \begin{cases} 1 & i = 1 \\ \angle\left(\sum\limits_{n=0}^{K-1} r(n - i\Delta) r^*(n)\right) & i = 2, \ldots, N-1 \end{cases}$$

$$\beta_i = \sqrt{\sum_{n=0}^{K-1} r(n - i\Delta) r^*(n - i\Delta - T_0)} \quad i = 1, \ldots, N-1$$

and K is the number of samples which are averaged and T_0 is one epoch interval.

Based on the different spatial characteristic of authentic and spoofing signals, the energy of spoofing signals from the same direction can be accumulated constructively while authentic signals from different directions can not. So the phase angles of vector $\mathbf{y}$ can be approximated as:

$$\begin{aligned} \theta_i &= \angle\left(\sum_{n=0}^{K-1} r(n - i\Delta) r^*(n)\right) \\ &\approx \angle\left(C_i \sum_{n=0}^{K-1} \left(\sum_{m=1}^{N_A} P_m^a a_{mi} + b_i \sum_{k=1}^{N_S} P_k^s\right)\right) \\ &\approx \angle\left(C_i b_i K \sum_{k=1}^{N_S} P_k^s\right) = \angle C_i + \angle b_i \end{aligned} \tag{56.9}$$

Based on the periodic characteristic of the PRN codes in the signals, the amplitude of vector $\mathbf{y}$ can be approximated as:

$$\begin{aligned} \beta_i &= \sqrt{\sum_{n=0}^{K-1} r(n - i\Delta) r^*(n - i\Delta - T_0\Delta)} \\ &\approx |C_i| \cdot \left(K\left(\sum_{m=1}^{N_A} P_m^a + \sum_{k=1}^{N_S} P_k^s\right)\right) \triangleq q|C_i| \end{aligned} \tag{56.10}$$

Taking Eqs. (56.9) and (56.10) into Eq. (56.8), the assumed vector $\mathbf{y}$ can be written as:

$$\mathbf{y} = \begin{bmatrix} q \\ q|C_2|e^{j(\angle C_2 + \angle b_2)} \\ \vdots \\ q|C_N|e^{j(\angle C_N + \angle b_N)} \end{bmatrix} = q\mathbf{C}\bar{b} = q\mathbf{b} \tag{56.11}$$

which concludes to a linear estimation of the spoofing SCV **b**.

56.3.2 Null Steering of the Synthesized Antenna Array

From Eq. (56.11), it is obvious that the orthogonal vector of vector **y** is orthographic to spoofing SCV. The orthogonal projection to the spoofing subspace can be obtained as:

$$P_{\perp} = I_N - \mathbf{y}\left(\mathbf{y}^H\mathbf{y}\right)^{-1}\mathbf{y}^H \tag{56.12}$$

so any vector in the subspace $P_{\perp}$ is orthographic to the vector **y** and also orthographic to the spoofing SCV **b**.

Taking an arbitrary vector **h** and define:

$$\mathbf{f} = P_{\perp}\mathbf{h} \in P_{\perp} \tag{56.13}$$

and the vector **f** is orthographic to the spoofing SCV **b**:

$$\begin{aligned} \mathbf{f}^H\mathbf{b} &= \mathbf{h}^H(P_{\perp})^H\mathbf{b} = \mathbf{h}^H P_{\perp}\mathbf{b} \\ &= \mathbf{h}^H\left(I_N - \mathbf{y}\left(\mathbf{y}^H\mathbf{y}\right)^{-1}\mathbf{y}^H\right)\mathbf{y}/d \\ &= \mathbf{h}^H\left(\mathbf{y} - \mathbf{y}\left(\mathbf{y}^H\mathbf{y}\right)^{-1}\mathbf{y}^H\mathbf{y}\right)/d \\ &= \mathbf{h}^H(\mathbf{y} - \mathbf{y})/d = 0 \end{aligned} \tag{56.14}$$

Applying the vector f to the synthesized antenna array output vector, the spoofing signals are removed from the original signals and an equivalent antenna direction pattern null is formed at the direction of spoofing signals:

$$\begin{aligned} v(n) &= \mathbf{f}^H\mathbf{R_N}(n) \\ &= \sum_{m=1}^{N_A}\mathbf{h}^H P_{\perp}\mathbf{a_m}\sqrt{P_m^a}F_m^a(n) \\ &\quad + \mathbf{h}^H P_{\perp}\mathbf{b}\sum_{k=1}^{N_S}\sqrt{P_k^s}F_k^s(n) + \mathbf{h}^H P_{\perp}\boldsymbol{\eta}(n) \\ &\approx \sum_{m=1}^{N_A}\mathbf{h}^H P_{\perp}\mathbf{a_m}\sqrt{P_m^a}F_m^a(n) + \mathbf{h}^H P_{\perp}\boldsymbol{\eta}(n) \end{aligned} \tag{1.15}$$

v(n) is the signal sequence after spoofing mitigation, and can be fed to the conventional GNSS receivers.

56.3.3 Structure of Anti-spoofing Receivers

An anti-spoofing receiver structure based on the proposed technique above can be configured as (Fig. 56.3):

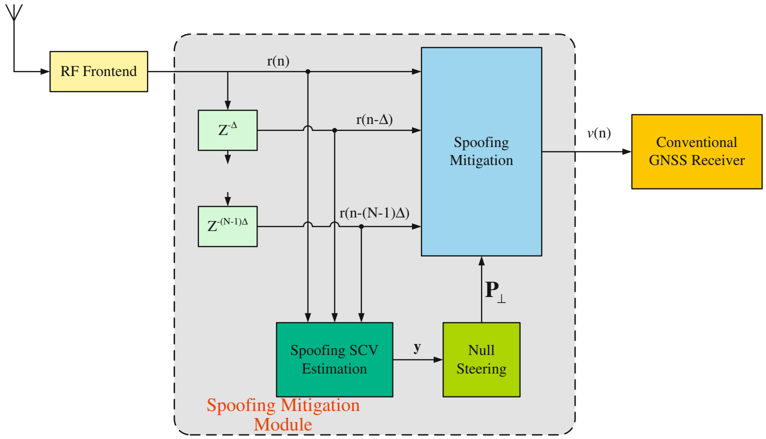


Fig. 56.3 Configuration of anti-spoofing GNSS receiver

56.4 Simulation Results

A simulation environment based on Matlab is setup to verify the effectiveness of the proposed anti-spoofing technique. Herein, four authentic and nine spoofing GPS L1 C/A PRNs are simulated, with CNRs (carrier power-to-noise density ratio) at 45 and 47dBHz respectively, while the velocity of receiver is 30 m/s and a two-element antenna array is synthesized.

Figures 56.4 and 56.5 show the cross ambiguity functions (CAF) for a certain PRN code before and after spoofing mitigation. It is observed that before spoofing mitigation (Fig. 56.4) there are two remarkable signal peaks in the time–frequency space and the authentic signal peak is weaker than the spoofing one, which could induce to a mistake signal acquisition. After spoofing mitigation (Fig. 56.5), it is obvious that only the authentic signal peak is reserved in the time–frequency space, which prevents the conventional receiver being affected by the spoofing interfere.

Fig. 56.4 CAF before spoofing mitigation

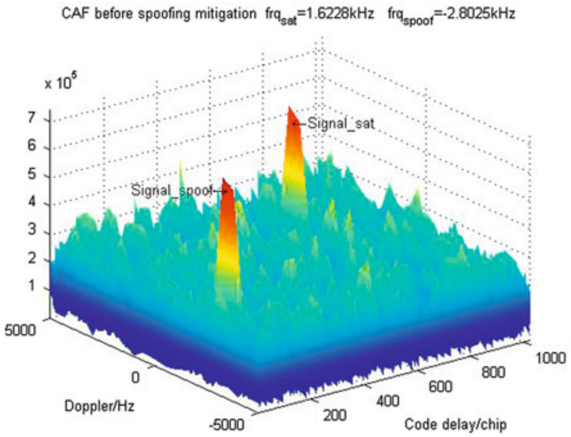
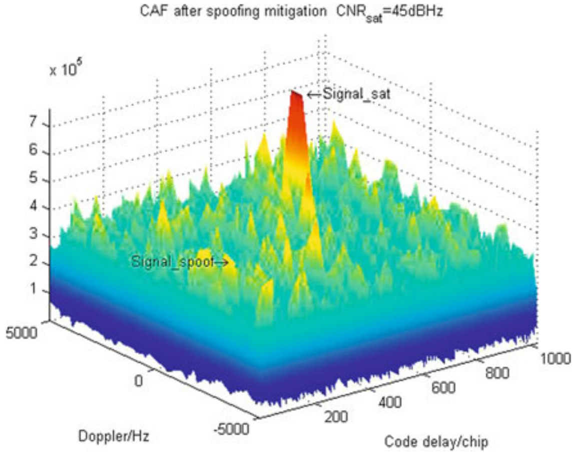


Fig. 56.5 CAF after spoofing mitigation



It can also be observed by compare the Figs. 56.4 and 56.5 that after spoofing mitigation, the noise floor of the CAF increases obviously, which results in 2 dB deterioration in the CNR of the authentic signal. Lightening the deterioration of spoofing mitigation to the authentic signals would be a major future work.

56.5 Conclusions

A low complexity spoofing mitigation method based on a moving antenna is proposed in this paper, which could effectively mitigate the spoofing signals from a point transmitter. The advantages in receiver cost and size make it suitable in civil navigation and timing domain.

References

1. Basker S (2010) Jamming: a clear and present danger. GPS World 21(4):8–9
2. Volpe JA (2001) Vulnerability assessment of the transportation infrastructure relying on the global positioning system. National Transportation Center, p 8
3. Broumandan A, Lin T, Moghaddam A, et al. (2007) Direction of arrival estimation of GNSS signals based on synthetic antenna array. In: Proceeding of ION GNSS 2007, pp 728–738
4. Pozzobon O (2011) Keeping the spoofs out. Inside GNSS 6(3):55
5. Wesson K, Shepard D, Humphreys T (2012) Straight talk on anti-spoofing. GPS World 23(1):32–39
6. Jafarnia-Jahromi A, Nielsen J, Lachapelle G (2012) GPS spoofer countermeasure effectiveness based on using signal strength, noise power and C/No observables. Int J Satell Commun Network 30:181–188
7. Daneshmand S, Jafarnia-Jahromi A, Lachapelle G (2012) A low-complexity GPS anti-spoofing method using a multi-antenna array. in: Proceeding of ION GNSS 2012