ATLANTIS PRESS

Advances in Engineering Research, volume 138

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

GNSS Spoofing Detection Using Pseudo-range Single Difference between Two Receivers

Ling Xiao [1,2,a,*], Xushuai Li[2,b], Yiming Zeng[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] xusmli@mail.ustc.edu.cn, [c]yiming_4528@qq.com

Keywords: GNSS Spoofing Interference, Pseudo-range Single-difference, Signal-in-space Properties

Abstract: The spoofing interference can mislead target receiver in reporting wrong position and time, it is a serious threat to the security of global navigation satellite system (GNSS) applications. The paper proposed an anti-spoofing method using the pseudo-range single-difference (PRSD) measurements of two receivers; the method recognizes spoofing signal by analysing the signal-in-space properties. Under the assumption that all the spoofing signals generating from the same antenna, their incident directions are same. However, the signals' incident directions are different for spoofing-free case, as they come from different satellites. Based on this difference, a spoofing decision variable is deduced. And the statistical characterization of the variable is analysed. In the last, the spoofing detection performance is evaluated by Monte-Carlo simulations. When the baseline is 2 meter long, the simulation results illustrated that if the false alarm rate is 0.01, the spoofing detection probability is up to 99%.

1. Introduction

The position, velocity and time (PVT) services, provided by GNSS, have a large inference in our daily life. Nowadays, various civilian applications such as aircraft navigation and landing systems, electrical power distribution grids, digital communication networks, stock exchange transactions, police and rescue services and many more are relying on GNSS signals. With the deeply using of GNSS, the security of the services is becoming more and more important. However, as the signals become extremely weak when it reaches the earth, they are vulnerable to interference. In addition, because the working frequency band, the modulation type, the civilian pseudo-random noise (PRN) codes and data information are public, the GNSS signals can be easily faked.

The counterfeit signals are termed spoofing interference. Among all the types of interference, the spoofing one is most harmful, as it can fool the target receiver report wrong position, time results without perception which may lead to serious consequences, such as leading unmanned aerial vehicle (UAV) off course [1], blocking digital communication networks [2], inducing power grids equipment failure [3] and so on.

Therefore researchers proposed many anti-spoofing techniques. All the techniques recognize spoofing signals by analysing difference between the authentic signal and the counterfeit one. With the assumption that all counterfeit signals born by one antenna, the spatial distribution of fake signals is very different from authentic ones. Because all the fake signals arrive from the same direction; while authentic signals born by different satellites, arriving from different directions. Based on this feature, Montgomery [4] have proposed a spoofing detection technique by comparing the calculated phase difference and the theoretical one of two fixed GNSS antennas, this technique requires a calibrated antenna array and it takes about one hour to do the detection. Borio [5] designed a double antenna receiver and developed a phase only analysis of variance (PANOVA) method in order to detect the phase difference coherency of spoofed PRN signals, this method can effectively recognize spoofing signals when the SNR (signal noise ratio) is larger than 10dB,

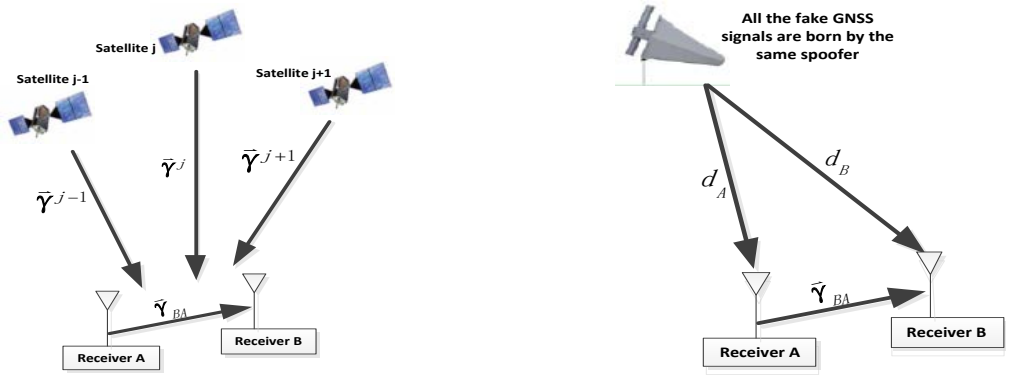
otherwise the detection performance is poor. Swaszek [6] designed a multi-receiver system which detects spoofing by checking the position result of the receivers, if the system is spoofed, all receivers will obtain same position result, in order to detect spoofing successfully it requires the distance between receivers at least large than twice position solution and that all the receivers are spoofed.

In this paper, a spoofing detection method is proposed which is also based on the signal spatial distribution difference mentioned above. However, the spoofing decision variable is constructed using pseudo-range measurements from two receivers in a PRSD-type calculation. It will be shown in the following section that the received signals can be checked in a short duration, thus the method may detect the spoofing signals in time. Also the method can be conducted even when the received signal is poor, as long as we can get the pseudo-range of the signal. Comparing with reference [6] a short baseline (such as 1 meter) is enough to get a good detection performance for the proposed method.

The rest of the paper is organized as follows: the PRSD measurement model was analysed firstly in section 2. In section 3, the spoofing decision variable is derived and its statistical characterization is analysed. The simulations are conducted in section 4 to evaluate the detection performance. In the last, the conclusion is drawn in section 5.

2. PRSD Measurement Model

In the section, the PRSD measurement models of the spoofing-free case and spoofed case are analysed respectively.



(a) The spoofing-free case (b) The spoofed case

Figure 1 Illustration of signal geometry distribution and dual-receiver spoofing detection system

2.1. PRSD Measurement Model of Spoofing-free Case

The signal-in-space property of authentic signals is illustrated in Fig.1 (a). The un-spoofed PRSD measurement model takes the form:

$$\Delta\rho_{BA}^{i}(k)=\rho_{B}^{i}(k)-\rho_{A}^{i}(k)=d\cdot\vec{\gamma}_{BA}^{T}(k)\cdot\vec{\gamma}^{i}(k)+c\left(dt_{B}(k)-dt_{A}(k)\right)+n^{i}(k) \tag{1}$$

where k represents the time instant. ρ_A^i, ρ_B^i are the pseudo-range from satellite i to receiver A and B respectively. d is the receiver baseline length. As d is short than 1Km, the ionosphere delay and troposphere delay can be assumed identical during the signal travelling arrival the two receivers, and the signal arrival direction to the two receivers can be assumed same. $\vec{\gamma}^i, \vec{\gamma}_{BA}$ are both unity vector in the reference coordinate system, $\vec{\gamma}^i$ denotes the signal steering vector from satellite i to the detection system, and $\vec{\gamma}_{BA}$ is the vector from receiver A to receiver B. c is the light velocity. dt_A and dt_B are the clock bias of receiver A and B respectively. n^i is measurement noise, which is a zero mean Gaussian variable, and the square root of variance is σ^i.

2.2. PRSD Measurement Model of Spoofed Case

The signal-in-space property of spoofing signals is illustrated in Fig.1(b). The spoofed PRSD measurement model is:

$$\Delta\rho_{BA}^{i}(k)=\left(d_B(k)-d_A(k)\right)+c\left(dt_B(k)-dt_A(k)\right)+n^i(k)=\beta_s(k)+n^i(k) \tag{2}$$

$$\beta_s(k)=\left(d_B(k)-d_A(k)\right)+c\left(dt_B(k)-dt_A(k)\right) \tag{3}$$

where d_A, d_B are the distance of spoofing transmitter antenna to receiver A and B antenna respectively. β_s integrates the geometric term and the clock bias term. This lumping together of unknowns is reasonable because none of the terms on the right-hand side of Eq. (3) depends on the satellite identifier superscript i.

3. Spoofing Decision Variable

It is shown in Eq. (1) and (2) that the means of PRSD measurement different authentic signals are different, while they are same for all the spoofing signals. It is a significant difference between the spoofing-free and spoofed case, which can be used to detect spoofing signals. In the following, the spoofing decision variable is deduced based on generalized likelihood ratio (GLRT) criterion. And the statistical characterization of the spoofing decision variable is analysed.

3.1. Derivation of spoofing decision variable

Before the derivation, the PRSD measurements are transformed by filtering, to improve the measurement's precision. That is

$$\Delta\rho_{BA}^{i}=\frac{1}{K}\sum_{i=1}^{K}\Delta\rho_{BA}^{i}(k) \tag{4}$$

where K is the filter length.

For spoofing-free case, putting (1) in (4), we get

$$\begin{aligned}\Delta\rho_{BA}^{i}&=\frac{d}{K}\sum_{k=1}^{K}\left(\vec{\gamma}_{BA}^{T}(k)\cdot\vec{\gamma}^{i}(k)\right)+\frac{c}{K}\sum_{k=1}^{K}\left(\left(dt_B(k)-dt_A(k)\right)\right)+\tilde{n}^i\\&\approx d\cdot\vec{\gamma}_{BA}^{T}(k)\cdot\vec{\gamma}^{i}(k)+c\left(dt_B(k)-dt_A(k)\right)+\tilde{n}^i\end{aligned} \tag{5}$$

where $\tilde{n}^i=\frac{1}{K}\sum_{k=1}^{K}n^i(k)$, it is a zero mean Gaussian variable, and the square root of variance is $\tilde{\sigma}^i=\frac{\sigma^i}{\sqrt{K}}$. The approximately equal at the second line bases on the assumption that the changing of the parameters $\vec{\gamma}^i, \vec{\gamma}_{BA}, dt_A$ and dt_B are negligible during filtering. It is reasonable when K is not very large. For example when the pseudo-range rate is 10Hz, if $K=10$, the filtering duration is 1 second. The changes of the above mentioned parameters are very small during 1 second.

For the spoofed case, we can get the identical result, that is

$$\Delta\rho_{BA}^{i}=\beta_s(k)+\tilde{n}^i \tag{6}$$

For the sake of simple expression, the spoofing decision variable is deduced using the normalized $\Delta\rho_{BA}^{i}$. That is

$$p^i=\frac{\Delta\rho_{BA}^{i}}{\tilde{\sigma}^i}=\mu^i+n \tag{7}$$

where μ^i denotes the mean of $\frac{\Delta\rho_{BA}^i(k)}{\tilde{\sigma}^i}$, n is normalized Gaussian variable.

Upon the equations (5) and (6), the spoofing detection hypothesis is

$$\begin{cases} H_0(spoofed) & :\forall i,j \quad \mu^i = \mu^j \\ H_1(spoofing-free) & :\exists i,j \quad \mu^i \neq \mu^j \end{cases} \tag{8}$$

In order to compute the GLRT, the joint probability density function (pdf) of the observed variables is required. More specifically the joint pdf of the p^i is given by

$$f(\mathbf{p}) = \frac{1}{(2\pi)^{N/2}} \exp\left\{ -\frac{1}{2} \sum_{i=1}^{N} \left(p^i - \mu^i \right)^2 \right\} \tag{9}$$

where $\mathbf{p} = \left[p^1, p^2, \cdots, p^N \right]^T$, N is the number of received signals.

Then the decision variable of the GLRT can be written as

$$l(\mathbf{p}) = \frac{\max_{\mu^1,\mu^2,\ldots,\mu^N} f(\mathbf{p} \mid H_1)}{\max_{\mu} f(\mathbf{p} \mid H_0)} \tag{10}$$

After calculating and simplification, the spoofing decision variable is

$$l(\mathbf{p}) = \sum_{i=1}^{N} (p^i - \hat{\mu})^2 \tag{11}$$

where $\hat{\mu} = \frac{1}{N} \sum_{i=1}^{N} p^i$.

3.2. Statistical characterization of the spoofing decision variable

For the spoofed case, it is obvious that $p^i - \hat{\mu}$ is a normalized Gaussian variable. Therefore $l(\mathbf{p})$ is a central chi-squared random variable with $N-1$ degrees of freedom. The one degree lose is due to the averaging of p^i.

For spoofing-free case, $p^i - \hat{\mu}$ is a non-zero mean Gaussian variable, and its variance is 1. Thus $l(\mathbf{p})$ is a non-central chi-squared random variable with $N-1$ degrees of freedom. And the non-central parameter is $\lambda = \sum_{i=1}^{N} \tilde{\mu}^{i2}$, $\tilde{\mu}^i$ is the mean of $p^i - \hat{\mu}$.

We use Neyman-Pearson criterion to determine decision threshold. As the pdf $f(x \mid H_1)$ of $l(\mathbf{p} \mid H_1)$ is relevant with the geometry position of satellites, $f(x \mid H_1)$ is difficult to determine. While the pdf $f(x \mid H_0)$ of $l(\mathbf{p} \mid H_1)$ is easy to compute, we choose to use the missing probability of H_0 to determine decision threshold. That is

$$P\left(l(\mathbf{p}) > T \mid H_0\right) = \alpha \tag{12}$$

where P is probability. α is the missing probability of H_0 and T is the threshold to be computed. If the decision variable is lower than T, then H_0 is accepted. If the converse is true, H_0 is rejected in favor of H_1. The spoofing signals detection probability P_d and false alarm probability P_f are

$$\begin{cases} P_d = \int_0^T f\left(x \mid H_0\right) dx = 1-\alpha \\ P_f = \int_0^T f\left(x \mid H_1\right) dx \end{cases} \tag{13}$$

4. Simulations

According to (15), the spoofing detection performance is determined by non-central parameter λ, which is relevant with the parameters σ^i, d, K and N. To verify the influence of the above four parameters on the detection performance, we simulate the receiver operation character (ROC) using Monte Carlo simulations. Corresponding to the four parameters, we set up three simulation tests. For each test only one parameter is changing, the other three is constant. Each test runs 10^6 times. The receiver direction vector is set as $\bar{\gamma}_{BA} = [1,0,0]^T$. Thus

$$\bar{\gamma}_{BA}^T(k) \cdot \bar{\gamma}^i(k) = \cos\varepsilon_i \cos\theta_i \qquad (14)$$

where ε_i, θ_i are the azimuth and elevation of the i th satellite. Under normal conditions the signals can arrive from arbitrary directions, and the angles $\{\varepsilon_i\},\{\theta_i\}$ can be reasonably modelled as uniform random variables with support[0,360°] and [0,90°] respectively.

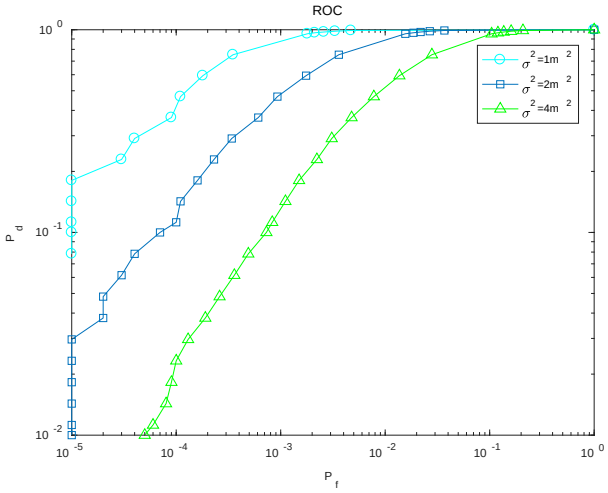


Figure 2 The simulation results for the scenario that $\sigma^2 = 1,2$ or 4 m^2, $d = 1m$, $K = 10$, $N = 4$.

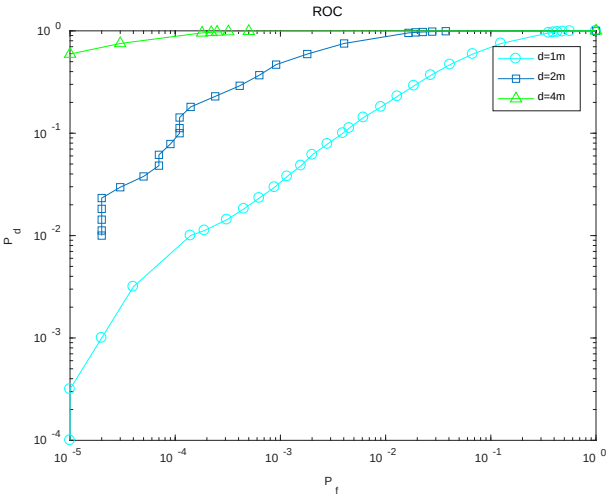


Figure 3 The simulation results for the scenario that $\sigma^2 = 2m^2$, $d = 1,2$ or 4 m, $K = 10$, $N = 4$

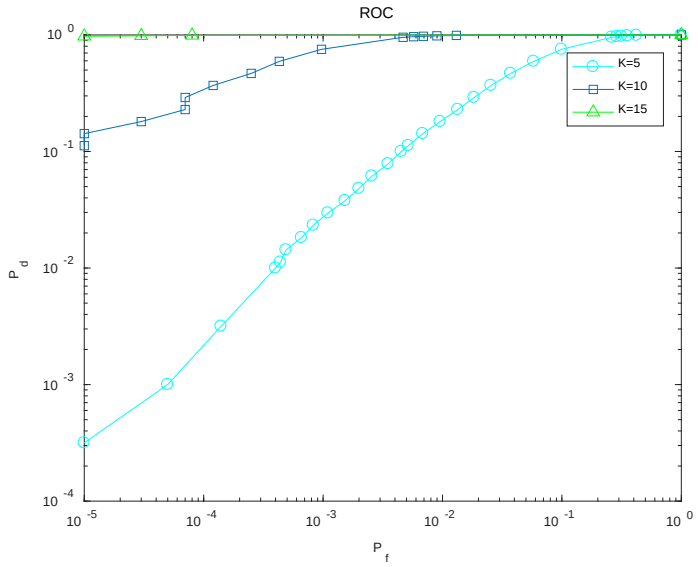


Figure 4 The simulation results for the scenario that $\sigma^2 = 2m^2$, $d = 1m$, $K = 5,10$ or 15, $N = 4$

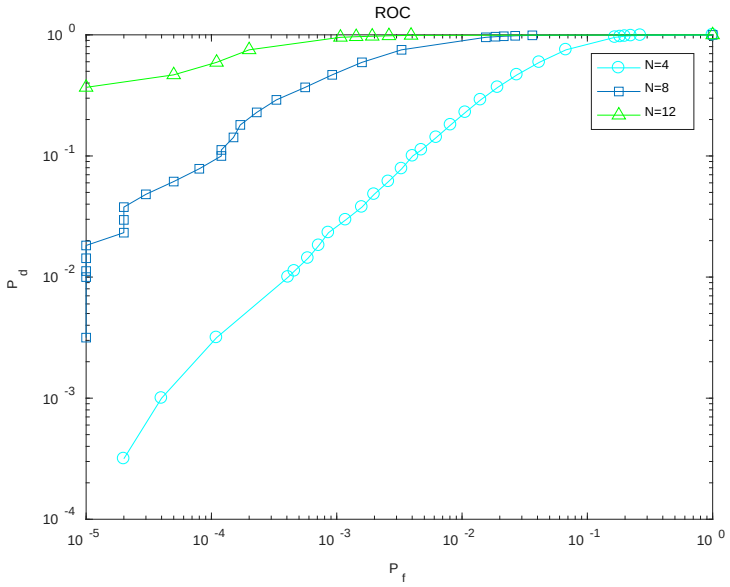


Figure 5 The simulation results for the scenario that $\sigma^2 = 2m^2$, $d = 1m$, $K = 10$, $N = 4,\ 8$ or 12

From the simulation results shown in figure 3 to figure 5, we can get that

1) When fixed other parameters, considering one parameter only, the smaller the noise variance σ^i, the longer the receiver baseline length d, the longer the filter length K, the more the number of satellites, the better the detection performance.

2) In consideration of the noise and satellite number are changing with time and surroundings, we can improve detection performance by increasing the receiver baseline length or increasing the filter length.

5. Conclusion

The spoofing interference is a serious threat to GNSS application security. The paper proposes a dual-receiver anti-spoofing technique using PRSD measurements, which can detect spoofing signals effectively when the two receivers are putting at a proper distance. This technique can be used in the digital communication network, smart grid to insure the security of GNSS timing service. And it also can be used in transportation to insure the security of GNSS navigation service, only if the platform is longer enough.

References

[1] Humphreys, T. UAVs Vulnerable to Civil GPS Spoofing [EB]. http://gpsworld.com. 2012.

[2] Recommended Minimum Performance Standards for cdma2000 Spread Spectrum Base Stations, C.S0010-B[R].Tech. rep., 3rd Generation Partnership Project 2 “3GPP2”, Feb. 2004.

[3] 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.

[4] Montgomery, P.Y., T.E. Humphreys, and B.M. Ledvina. “Receiver-Autonomous Spoofing Detection: Experimental Results of a Multi-antenna Receiver Defense Against a Portable Civil GPS Spoofer”.in Proceedings of ION ITM 2009, Jan 26-28, 2009, Anaheim, CA,pp. 124-130.

[5] Borio, D. “PANOVA Tests and their Application to GNSS Spoofing Detection”.in IEEE Transactions on Aerospace and Electronic Systems, vol. 49, no. 1, January, 2013, pp. 381-394.

[6] Swaszek, P. F., R. J. Hartnett, M. V. Kempe, and G. W. Johnson. “Analysis of a Simple, Multi-Receiver GPS Spoof Detector”. in Proceedings of the 2013 International Technical Meeting of The Institute of Navigation, Jan. 29 – 27, 2013, San Diego, CA, pp. 884-892.