

A Suppression Method against Spoofing Jamming based on Multipath Fading Detection

Xue Li^{1,*}, Linshan Xue²

¹University of Electronic Science and Technology of China, Chengdu, China

²University of Electronic Science and Technology of China, Chengdu, China

*Corresponding author e-mail: lixue.1981@hotmail.com

Abstract. Today's interference methods to the receiver include human jamming and non-human interference, and the human one can be divided into two types — suppressing jamming and spoofing jamming. In the spoofing jamming, the jamming source transmits or generates interference signal, trapping the receiver into a wrong location and time estimation of signals from receiving the real signal. Due to its strong similarity to the real one, the interference signal is difficult to be detected and suppressed by the receiver. Thanks to the similarity between spoofing jamming signal and multipath signal, the thesis aims to improve and optimize the WRELAX algorithm — by detecting and identifying signals after WRELAX algorithm according to the multipath fading, we can, finally, separate the spoofing jamming signal and real signal.

1. Introduction

Among the main human interference signals, there are two major types of jamming to satellite signals including suppressing and spoofing jamming. The former prevents the receiver from receiving the low-power GNSS satellite signal by increasing the power of the interference signal. Main algorithms at present against suppressing method involve time/domain filtering, spatial filtering and joint filtering technology, which are gradually maturing. And in the latter one, spoofing jamming, the jammer transmits the original satellite signal, or generates a similar signal locally by itself, so that the receiver is cheated by the signal with a different location and time information from the real signal [1]. If this interference signal is not detected and removed in time, it will lead to a great impact on the receiver's security. Moreover, the strong similarity of the spoofing jamming signal to the real signal throws the receiver into a great confusion, which harms a lot. In the current suppression algorithm against spoofing jamming, based on the rule that the interference signal generally bears a power about 2 dB higher than the original satellite signal, we can estimate its amplitude and direction, so as to construct the orthogonal complementary space projection matrix of jamming subspace, and project the array receiving signal. However, this method has two disadvantages: firstly, to estimate the amplitude and direction, we need to use the RELAX algorithm, which demands a hard computation and increasing needed resources; secondly, the power of the spoofing jamming signal is not quite distinct from the satellite signal and can be almost the same as the original one after transmission and attenuation. In this case, sometimes the power detection does not get an accurate result, which finally leads to a great error in constructing the jamming subspace.



By contrast, in the non-human interference, the multipath signal is an interference signal received after being reflected by objects surrounding the receiver antenna, which results in the distortion of the chip, and ultimately changes the phase discrimination characteristics of the receiver tracking loop, causing tracking and measuring errors. In essence, the signal after reflection changes in the phase and time delay, leading to the mistake after its superposition on the real one [5].

This paper puts forward a new algorithm: because changes in the phase delay and time delay are reasons for errors both in multipath signal and spoofing jamming signal, the thesis uses WRELAX algorithm[2] to estimate the code time delay and power of spoofing jamming signal, as well as code time delay and power of the satellite signal. In this way, the spoofing interference signal can be recognized and separated according to different extents of attenuation by the ground reflection to the satellite signals with different heights.

2. Anti-jamming Algorithm

2.1. Data Model

When receiving the paper, we assume that the corresponding authors grant us the copyright to use the paper for the book or journal in question. Should authors use tables or figures from other Publications, they must ask the corresponding publishers to grant them the right to publish this material in their paper. The satellite-transmitted signal can be expressed as

$$s(t) = D(t)c(t) \cos(w_c t) \quad (1)$$

In the formula, $D(t)$ is the navigation message for satellite signals; $c(t)$ is the C/A code; w_c is carrier frequency.

Spoofing jamming creates jamming to satellite signal reception by advancing or delaying the satellite signal, which is reflected in the time domain as advance or delay and phase shift. Spoofing jamming is divided into transmitting spoofing jamming and generating spoofing jamming: the former one can produce wide impact to more facilities and cause time delay compared to the real signal; by contrast, the latter generating one can only lead to interference to civilian facilities, but the military equipment is free from its interference in the advantage of its more confidential spreading code information. Therefore hereof we develop a discussion on transmitting spoofing jamming with a wider impact, which features in a time delay compared to the real signal [2]~[4]. Assuming the received signal can be represented as

$$s_r(t) = \sum_{p=0}^P \tilde{\alpha}_p D(t - \tau_p) c(t - \tau_p) \cos(w_c(t - \tau_p) + \tilde{\varphi}_p) + e(t) \quad (2)$$

Where $\tilde{\alpha}_p$, τ_p , $\tilde{\varphi}_p$ stand for the amplitude, delay and initial phase of the PTH signal separately. And $p=0$ represents direct satellite signal. The symbol $e(t)$ represents the thermal noise. The navigation period is far larger than the C/A code period, and estimation of subsequent time delay requires short data block length (only a few C/A code period). Here we assume that $D(t - \tau_p) = 1$ without changes during the duration of the data, and Eq. (2) can be simplified as Eq. (3).

$$s_r(t) = \sum_{p=0}^P \alpha_p c(t - \tau_p) \cos(w_c(t - \tau_p) + \tilde{\varphi}_p) + e(t) \quad (3)$$

Assuming the carrier and doppler frequency can be obtained accurately, signal after carrier loop demodulation can be written as:

$$\tilde{s}_r(t) = \sum_{p=0}^P \alpha_p c(t - \tau_p) \cos(\phi_p' - \phi_0') + e(t) \quad (4)$$

The symbol ϕ_p' is the phase of the spoofing signal or multipath signal. ϕ_0' means the estimated value of the carrier phase of the direct signal

$$s_r(t) = \sum_{p=0}^P \alpha_p c(t - \tau_p) \cos(\phi_p' - \phi_0') + e(t) \quad (5)$$

After Hilbert transformation and sampling, Eq. (5) can be written as Eq.(6)

$$\tilde{s}_r(nT_s) = \sum_{p=0}^P \tilde{\alpha}_p c(nT_s - \tau_p) + \tilde{e}(nT_s), n = 1, 2, \dots, N \quad (6)$$

Where T_s is the sampling interval and N is the total number of samples. For a further analysis, we replace $\phi_p' - \phi_0'$ by ϕ_p , and $\alpha_p \exp(j\phi_p)$ by $\tilde{\alpha}_p$.

In Eq. (6), the parameters to be estimated are $\{\tilde{\alpha}_p, \tau_p\}$, $p = 1, 2, \dots, P$. In order to further analyze and obtain the time delay parameters, we apply the Discrete Fourier Transform (DFT) to Eq. (6)

$$X(k) = C(k) \sum_{p=0}^P \tilde{\alpha}_p e^{jw_p k} + E(k), -N/2 \leq k \leq N/2 - 1 \quad (7)$$

Where $X(k)$, $C(k)$ and $E(k)$ are the DFT of $x(n)$, $c(n)$, $e(n)$. $w_p = -2\pi\tau_p f_s / N$; f_s stands for the sampling interval.

2.2. WRELAX Algorithm

In order to obtain the estimated value, we define the nonlinear least squares cost function as followed

$$Q_1(\{\tilde{\alpha}_p, \tau_p\}_{p=0}^P) = \sum_{k=-N/2}^{N/2} \left| X(k) - C(k) \sum_{p=0}^P \alpha_p e^{jw_p k} \right|^2 \quad (8)$$

Where

$$C = \text{diag}[C(-N/2), C(-N/2+1), \dots, C(N/2-1)] \quad (9)$$

$$X = [X(-N/2), X(-N/2+1), \dots, X(N/2-1)] \quad (10)$$

$$a(w_p) = [e^{jw_p(-N/2)}, e^{jw_p(-N/2+1)}, \dots, e^{jw_p(N/2-1)}] \quad (11)$$

Minimizing Eq. (7) and assuming that all non P terms have been estimated, we define

$$X_p = X - \sum_{\substack{q=0 \\ q \neq p}}^P \tilde{\alpha}_q [Ca(w_p)] \quad (12)$$

Insert the Eq. (7) into Eq. (8)

$$Q_2(\tilde{\alpha}_p, \tau_p) = \|X_p - \alpha_p Ca(w_p)\|^2 \quad (13)$$

Then minimize the cost function of Eq. (13), we get equations below

$$\hat{w}_p = \arg \max_{w_p} |a^H(w_p)(C^* X_p)|^2 \quad (14)$$

$$\hat{\alpha}_p = \frac{a^H(w_p)(C^* X_p)}{\|C\|_F^2} \bigg|_{w_p = \hat{w}_p} \quad (15)$$

Where $\|\bullet\|_F^2$ stands for Frobenius norm. \hat{w}_p can be obtained from the dominant peak of the periodogram $|a^H(w_p)(C^* X_p)|^2$ which can be realized by one dimension non complementary FFT operation. $\hat{\alpha}_p$ Stands for the complex amplitude of $\frac{a^H(w_p)(C^* X_p)}{\|C\|_F^2}$

Assuming that there is a direct satellite signal and a spoofing jamming, the estimation of $\{\hat{\alpha}_p, \hat{w}_p\}_{p=0}^I$ can be achieved through the following steps:

Step (1) Assuming that there is only direct signal, using X_0 to estimate $\{\hat{\alpha}_0, \hat{w}_0\}$ by Eq. (14) and Eq. (15)

Step (2) Computing X_I by $\{\hat{\alpha}_0, \hat{w}_0\}$ and Eq (12), using X_I to estimate $\{\hat{\alpha}_I, \hat{w}_I\}$ by Eq. (14) and Eq. (15)

Step (3) Using $\{\hat{\alpha}_I, \hat{w}_I\}$ and Eq. (12) to re-estimate X_0 , and X_0 to re-estimate $\{\hat{\alpha}_0, \hat{w}_0\}$ by Eq.(14) and Eq.(15). Repeat the above steps until convergence.

Above steps can be expanded to any cases with the presence of more spoofing jamming sources.

2.3. Discrimination of spoofing jamming

In the analysis, we take flat terrain as an example (with the earth curvature ignored) based on the presumption of a uniform space environment illustrate the effect of reflection on satellite signal.

According to Huygens principle, in the construction of satellite communication lines, part of satellite signals can be projected to the ground. So except for those direct signals, some signals reflected by the ground in a certain condition will also reach the receiver. As shown in the figure 1.

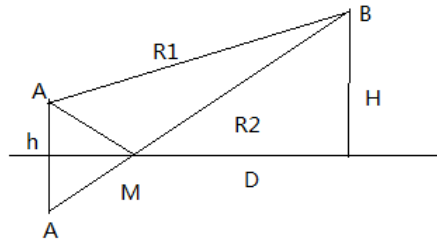


Figure 1. Multipath fading model

Considering only one reflected signal and one direct signal entering the receiving antenna, and assuming a smooth, flat ground, the reflection of the satellite signal can be seen as a specular reflection. In addition, here we ignore the air's refraction and scattering of the signal, and get the multipath fading model in Figure 1. In the figure, we use A for the receiving antenna on the ground, B for the transmitting antenna, M for the reflection point on the ground, h for the height of receiving antenna, H for the transmitting antenna height, and D for the horizontal distance between the receiving antenna and transmitting antenna. To normalize the direct and the reflected signals, we set the direct signal as 1, and the reflected signal as $\rho e^{j\theta}$, in which the ρ and θ represents for amplitude ratio and the phase difference between the reflected signal and the direct signal. Data of the reflection coefficient ρ mainly relates with the ground, and alters with the beam angle of the receiving antenna. And data of θ mainly depends on the phase delay θ_m caused by the ground reflection and the phase difference θ_d produced by the difference of the propagation path between the direct and the reflected signals. $\theta = \theta_m + \theta_d$. On the condition of a low angle of pitch, when the incident signal forms a less-than-10-degree angle with the ground, $\theta_m \approx \pi$.

As is shown in Figure 1, the transmission path of the direct signal is $R_1 = AB$, and the transmission path of the reflected signal is $R_2 = AM + BM = A'B$, and A' is the mirror point relative to the ground at the A point. According to equations below:

$$R_1 = \sqrt{(H-h)^2 + D^2} \quad (16)$$

$$R_2 = \sqrt{(H+h)^2 + D^2} \quad (17)$$

We get the transmission path difference between the reflected signal and the direct signal, Delta R, as follows:

$$\Delta R = R_2 - R_1 = \sqrt{(H+h)^2 + D^2} - \sqrt{(H-h)^2 + D^2} = \frac{4hH}{\sqrt{(H+h)^2 + D^2} + \sqrt{(H-h)^2 + D^2}} \quad (18)$$

Because the height data of the receiver is far smaller compared with that of the satellite and its distance to the satellite,

$$\Delta R = \frac{2hH}{\sqrt{H^2 + D^2}} \approx \frac{2hH}{R_1} \quad (19)$$

The phase difference θ_d caused by the transmission path difference is as follows:

$$\theta_d = \frac{2\pi\Delta R}{\lambda} = \frac{4\pi hH}{\lambda R_1} \quad (20)$$

So we get

$$\theta = \frac{4\pi hH}{\lambda R_1} + \pi \quad (21)$$

In addition, $h \ll H$, so the reflection point M must be located near the ground station antenna A. Therefore, the topography and geomorphology near the ground station antenna A will pose a great influence on the reflection coefficient ρ . In this way, in the absence of spoofing jamming, the multipath environment generated by real satellite signals can be used to identify spoofing jamming signals.

Set E_0 as the field strength of the receiver satellite signal, and the value of the field intensity of the direct signal to the receiving point can be expressed as:

$$\theta = \frac{4\pi hH}{\lambda R_1} + \pi \quad (22)$$

The instantaneous value of the field intensity of the reflected wave is

$$e_2(t) = \rho E_0 \cos(\omega t - \theta - \frac{2\pi}{\lambda}(R_2 - R_1)) \quad (23)$$

Vector synthesis at A point is

$$\begin{aligned} \vec{E} &= \sqrt{E_0^2 + E_0^2 \rho^2 - 2E_0^2 \rho \cos\{\pi - [\theta_m + \frac{2\pi}{\lambda}(R_2 - R_1)]\}} \\ &= E_0 \sqrt{1 + \rho^2 + 2\rho \cos(\theta_m + \frac{2\pi}{\lambda}(R_2 - R_1))} \end{aligned} \quad (24)$$

Set the power ratio of the received signal of antenna to the direct signal as the fading depth L,

$$\begin{aligned} L = \frac{E}{E_0} &= 10 \log \left[\frac{1 + \rho^2 + 2\rho \cos(\theta_m + \frac{2\pi}{\lambda}(R_2 - R_1))}{2} \right] \\ &= 10 \log \left[\frac{1 + \rho^2 - 2\rho \cos(\frac{4\pi hH}{\lambda R_1})}{2} \right] \end{aligned} \quad (25)$$

When $\theta = (2n+1)\pi$, ($n=1, 2, 3, \dots$), the reflection signal bears an opposite phase to the direct signal. The signal received by the receiving antenna is the algebraic difference between the direct and reflected signals, and the fading depth L will reach its extreme value under such circumstance.

Apply $\theta = (2n+1)\pi$, ($n=1, 2, 3, \dots$) to Eq. (25)

$$R_1 = \frac{2hH}{n\lambda} \quad (26)$$

When the horizontal distance between the ground station and the satellite satisfies the Eq. (26), the depth of the fading depth L will get its extreme value, and the value of the fading depth of L depends on the value of the fading depth. At the same time, when the satellite signal comes to a certain value of wavelength λ , the extreme value, L , of the fading depth depends only on the data of the h and H . In the range of distance $15 \text{ km} \leq D \leq 115 \text{ km}$, based on the Eq.(26) we can attain the relationship between the fading depth L and the distance D .

3. Organization of the Text

When the spoofing jamming signal get a lower power than the real signal, it will produce the same impact as the multipath signal to the real signal. On this condition, we can estimate it by WRELAX algorithm. And in the case of a higher or same power, we discuss as follows: by simulation we generates satellite real signal and its multipath interference, as well as spoofing jamming and its multipath interference. Set the amplitude attenuation of multipath interference compared with the direct signal as 0.7, 0.8 separately, and the code delay as 1 chips, the simulation images can be shown in figure 2 and figure 3.

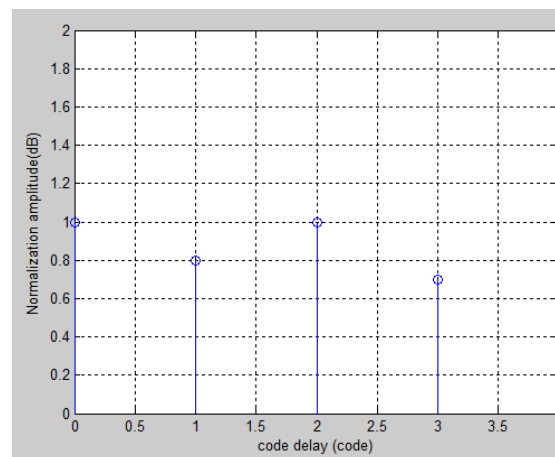


Figure 2. Estimation of amplitude and delay by WRELAX algorithm

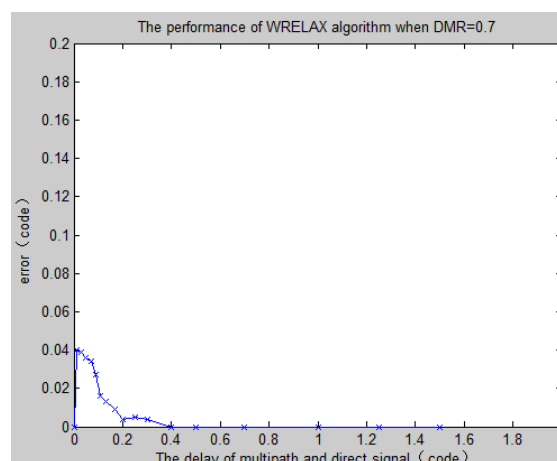


Figure 3. Estimation results of WRELAX algorithm with different time delay

Seeing from the figure, when the code delay between the multipath signal and the direct signal is 0.5, the WRELAX algorithm makes an excellent estimation of the delay and amplitude of the signal. In general, thanks to the multipath signal lagging behind the direct signal, we can distinguish the multipath signal from the direct signal. In the third section, it is known that satellite signals of different heights will produce different multipath signals near the receiver, and their fading factors are like figure 4.

The height of the satellite is 0~20000km. The distance between the satellite and the receiver is 0~30000km, the wavelength is 0.2, and the reflection coefficient is 0.9

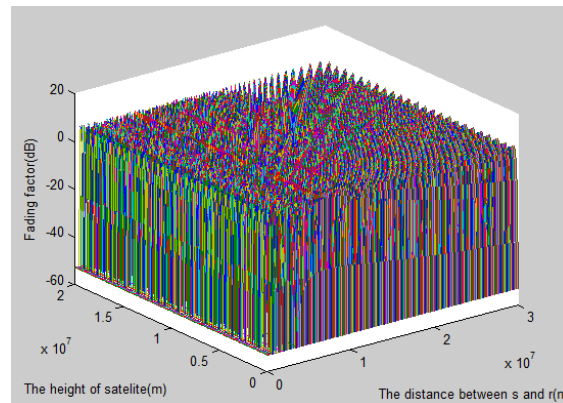


Figure 4. Fading factor of different height and different distance

The height of the satellite is 20000km. The distance between the satellite and the receiver is 0~30000km, the wavelength is 0.2, and the reflection coefficient is 0.9.

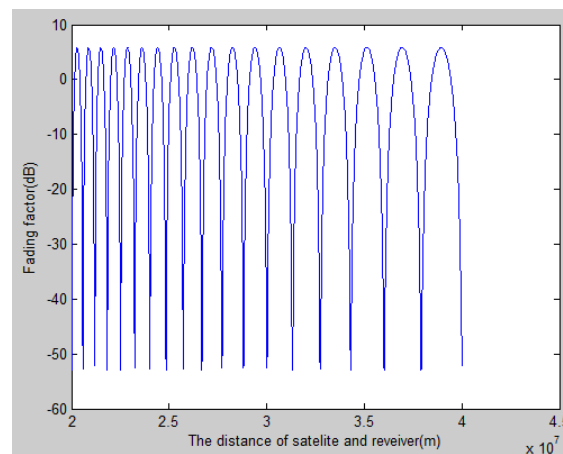


Figure 5. Fading factor of different distance

According to figure 5, different multipath signals generated near the receiver produce on different height of the transmitter. And the ratio value of multipath signal to direct signal varies with the distance between the satellite and the transmitter and the height of the transmitter, which can be described as above.

Based on the simulation figure 4 and 5, we can identify and suppress the spoofing jamming in the following way: the transmitter of spoofing jamming signal and that of the real signal are set as different heights generally, resulting in difference in multipath attenuation factor. Then after identifying power and time delay of signals based on WRELAX algorithm, we can distinguish multipath signals from direct signals. By calculation we get the ratio of direct signal to its multipath

signal, and then compare it with multipath attenuation factor near the receiver, finally we get the height of current transmitter. For a conclusion at the end, we compare the above height value with the signal transmitter height given by the satellite navigation message, define it as the real satellite signal when match but the spoofing jamming signal when it is not.

4. Conclusion

This thesis aims to estimate the time delay and power of signals reaching the receiver at the same time under the guidance of the WRELAX algorithm. Due to the height gap between satellite and deception jamming transmitters, as well as differences in distances of satellite and spoofing jamming to the receiver, multipath signals of different signals surrounding the receiver differs from each other in power and time delay. Then by detecting ground-reflected signals surrounding the receiver, we can get the image of the fading factor of multipath signal produced by the real signal in the case of jamming-free, and compare it with that under spoofing jamming, and those unmatched are recognized as jamming signals.

References

- [1] Mustapha Flissi, Khaled Rouabah, Djamel Chikouche. Performance of new BOC-AW-modulated signals for GNSS system [J]. EURASIP Journal on Wireless Communications and Networking, 2013: 1-8
- [2] Wu Renxi, Wang Wenyi, Lu Dan, Wang Wei, Jia Qiongqiong. Adaptive anti-jamming technology for satellite navigation [M]. Science Press, 2015.12
- [3] Ali Broumandan, Ali Jafarnia-Jahromi, Gerard Lachapelle, Rigas T. Ioannides. An approach to discriminate GNSS spoofing from multipath fading [J]. 2016 8th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC). Year: 2016 Pages: 1 – 10
- [4] Ali Broumandan, Ranjeeth Siddakatte, Gérard Lachapelle, An Approach to Detect GNSS Spoofing [J]. University of Calgary, Alberta Canada. Feature Article.
- [5] Xue Yong, Sun Bo, Zeng Xiaobing. Satellite communications anti-jamming technology analysis [J]. International Space, 2012. 8: 41-51