GPS Solutions (2018) 22:28
https://doi.org/10.1007/s10291-017-0693-7

ORIGINAL ARTICLE

GNSS spoofing detection based on new signal quality assessment model

Yanfeng Hu[1] · Shaofeng Bian[1] · Kejin Cao[1] · Bing Ji[1]

Received: 6 September 2016 / Accepted: 26 December 2017 / Published online: 2 January 2018

Abstract
Security exposure in satellite navigation has become a real threat in the face of increasing complexity of the electromagnetic environment. We propose a low-complexity authenticity verification technique by establishing a new model for signal quality assessment. This model is based on total signals energy measurement of both spoofing signals and authentic signals hereafter referred to as the TSEM method. The TSEM method does not rely on the movement of the user receiver or the assumption that all spoofing signals should come from only one transmitting antenna. Simulation results based on GNSS software verify the efficiency of the proposed method. The results show that this method can work well even when the received signal strengths of the spoofing and authentic signals are very close to each other. Also, the performance of spoofing detection gets better with increasing strength of the spoofing signal. This spoofing detection method can easily be applied on GNSS anti-spoofing receivers without changing the architecture of receivers since the characteristics are simple and effective. However, the performance of this method may deteriorate when the code phase differences between authentic signals and spoofing signals are < 1.5 chips and the Doppler frequency differences between authentic signals and spoofing signals are relatively small. But it is difficult to keep the code phases and Doppler frequencies accurately to meet the requirements for the spoofer to avoid being detected. Also, multipath signals effects can also be bad for the robustness of the TSEM method. Thus, the TSEM method needs to be integrated with some suppression technology to restrain or eliminate the multipath signals. Further research is needed to improve the robustness of this method.

Keywords Global navigation satellite systems · Receiver · Spoofing detection · Signal quality

Introduction

Global navigation satellite system (GNSS) plays an increasingly crucial role in numerous fields of application. In the past, users used to be concerned about availability and accuracy and ignore the safety which, however, gradually starts to get users attention.

Global navigation satellite system (GNSS) signals received by the user on earth surface are quite weak, which leads to potential vulnerability to interference. In 2001, United States Department of Transportation report highlighted the dangers of GNSS spoofing (Volpe 2001). With respect to traditional jamming, spoofing is a more sophisticated interference pattern that can make GNSS receivers indicate the incorrect position, velocity, and time by means of transmitting false GNSS-like signals. If the user receiver is unaware of this covert spoofing attack, it may cause great interference to the user receiver. Therefore, spoofing is much more dangerous than jamming (Psiaki and Humphreys 2016; Shaofeng et al. 2017).

Many spoofing countermeasure techniques have been proposed (Kuhn 2005; Bardout 2011). Some are based on encryption mechanism, like spreading cryptographic code measures (Humphreys 2013), or navigation message authentication measures (Wesson et al. 2012; Kerns et al. 2014). These are unpractical to be realized in a short period due to quite a high cost and complexity. O'Hanlon et al. (2010, 2012, 2013) provided a considerable analysis on codeless cross-correlation measures. Heng et al. (2015) extend the dual-receiver P(Y)-code correlation method to a network of receivers with higher availability.

Other countermeasure techniques are based on analyzing the abnormal features caused by spoofing attacks,

✉ Yanfeng Hu
daohang_yanfeng@163.com

[1] Department of Navigation Engineering, Naval University of Engineering, Wuhan 430033, China

such as clock error (Hwang and McGraw 2014; Jafarnia-Jahromi et al. 2013; Shepard et al. 2012), automatic gain control (AGC) (Akos 2012), signal quality (Broumandan et al. 2012; Dehghanian et al. 2012; Jafarnia-Jahromi et al. (2012, 2014)). Khanafseh et al. (2014) propose a method to detect GPS spoofing attacks using residual-based receiver autonomous integrity monitoring (RAIM) with inertial navigation sensors. Lee et al. (2015) puts forward a GNSS spoofing detection method aided by accelerometers. Psiaki et al. (2013, 2014) studied the use of multi-antenna technology against spoofing attacks.

As of today, there are no existing spoofing countermeasure techniques that can cope with all spoofing cases. Many countermeasures are confined to specific conditions. As for which kind of technique or techniques to adopt, the user receiver needs to take cost, complexity and other factors into account.

Jafarnia-Jahromi et al. (2012) have assessed the reduced effectiveness of the GPS spoofer countermeasure during acquisition when the GPS receiver utilizes C/N0 discrimination, which leads to the deterioration of the receiver detection performance. Also, the detection method based on C/N0 should get the accurate Doppler frequency and the code phase information through acquisition. Jafarnia-Jahromi et al. (2014) propose a low-complexity authenticity verification technique, by taking advantage of the GPS signal structure, which we refer to as the SPA method for short in the following presentation. However, through the TEXBAT processing results of the SPA method, we can find the test statistics fluctuate severely which means the signal energy may not be combined fully and makes the receiver detection performance worse (Jafarnia-Jahromi et al. 2014; Broumandan et al. 2015).

We present a new spoofing detection method based on total signals energy measurement of both spoofing signals and authentic signals (hereafter referred to as the TSEM method). Compared with traditional C/N0 detection method, this new technique does not need to know the Doppler frequency and code phase. This method has the same advantages as the SPA method such as being based on digital samples without despreading the received signal, and it does not need any information about the AGC gain. The TSEM method utilizes the pre-despreading concept, but its fundamental theory is totally different. Compared with the SPA method, this new signal quality assessment model, by adopting coherent integration theory, extracts all signals strength completely. This method fetches the total energy of authentic signals and spoofing signals through the new signal quality assessment model, using the cycle characteristics of C/A code, while the noise component is uncorrelated. The interference caused by a spoofing attack will reduce the SNR of authentic signals. While the test value related to the total energy of spoofing and authentic signals rises as the power of spoofing interference rises.

Received signal model

This section presents the received signal model based on the average GPS receiver, of which the basic structure is shown in Fig. 1. Take GPS L1 C/A code receiver as an example. Its internal structure can be divided into three parts: RF front-end processing stage, baseband digital signal processing stage, and navigation information output stage as shown in Fig. 1.

It is assumed that the structure of spoofing signals is similar to that of authentic signals. But as for the spoofing signals, the power level, code delay, Doppler frequency, navigation message may be different from those of the authentic signals.

Through down-conversion and A/D conversion, the received signal of a spoofing attack can be modeled as

$$r(nT_s) = S^a_{IF}(nT_s) + S^s_{IF}(nT_s) + \eta_0(nT_s) \tag{1}$$

$$S^a_{IF}(nT_s) = \sum_{i=1}^{M} \sqrt{P^a_i} D^a_i\left(nT_s - \tau^a_i\right) c_i\left(nT_s - \tau^a_i\right) e^{j\varphi^a_i + j2\pi(f_{IF}+f^a_{di})nT_s} \tag{2}$$

$$S^s_{IF}(nT_s) = \sum_{i=1}^{M} \sqrt{P^s_i} D^s_i\left(nT_s - \tau^s_i\right) c_i\left(nT_s - \tau^s_i\right) e^{j\varphi^s_i + j2\pi(f_{IF}+f^s_{di})nT_s} \tag{3}$$

where P^a_i and P^s_i are, respectively, the authentic signal power and the spoofing signal power. The superscript symbols "a" and "s," respectively, denote authentic and spoofing. $D_i(nT_s)$ denotes the transmitted navigation data bit, $c_i(nT_s)$ is the PRN sequence at a time instant nT_s, τ_i denotes the time delay, φ_i denotes the initial phase, f_{IF} means the center frequency of the baseband signals, f_d is the Doppler frequency shift, and T_s is the sampling interval. For analyzing conveniently and without loss of generality, it is assumed that the spoofing signal and authentic signal have the same satellites PRNs,

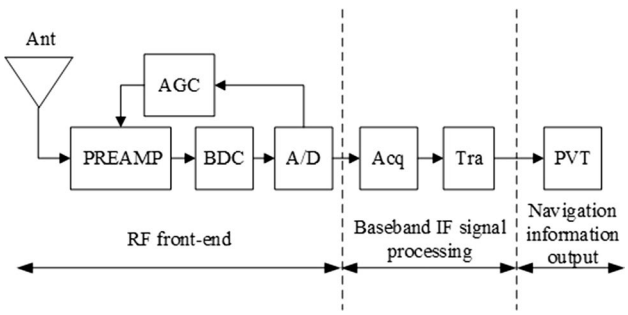

Fig. 1 Typical work process of single-frequency GPS receiver

the number of which is M. $\eta_0(nT_s)$ is complex additive white Gaussian noise with zero mean and the variance δ_0^2.

This next section introduces the received model with spoofing attack. Details of the subsequent sections are all based on this basic model.

Establishment of test quantity

This section presents the mechanism of the spoofing test quantity, which is the output of the spoofing detection mode. Here we establish a new variable $u[k, p]$, which is defined as:

$$u[k,p] = \frac{1}{N}\sum_{n=(k-1)N+1}^{kN} r(nT_s)\times r^*\left(nT_s - \frac{p}{2}T_c\right), \quad (0 < p < 2046) \tag{4}$$

where N means the number of consecutive samples of 1 ms, k means the kth coherent integration output result, and T_c is the chip period of C/A code.

When p equals 1, we can get $u[k, 1]$. Then, we can have an analysis of the characteristics of $u[k, 1]$, through calculating $r(nT_s)\times r^*(nT_s - 0.5T_c)$ as follows

$$\begin{aligned} r(nT_s)\times r^*(nT_s-0.5T_c) &= \left[S_{IF}^a(nT_s)+S_{IF}^s(nT_s)+\eta_0(nT_s)\right] \\ &\times\left[S_{IF}^{a*}(nT_s-0.5T_c)+S_{IF}^{s*}(nT_s-0.5T_c)+\eta_0^*(nT_s-0.5T_c)\right] \\ &= S_{IF}^a(nT_s)S_{IF}^{a*}(nT_s-0.5T_c)+S_{IF}^s(nT_s)S_{IF}^{s*}(nT_s-0.5T_c) && \text{I} \\ &+S_{IF}^a(nT_s)S_{IF}^{s*}(nT_s-0.5T_c)+S_{IF}^s(nT_s)S_{IF}^{a*}(nT_s-0.5T_c) && \text{II} \\ &+\left[S_{IF}^a(nT_s)+S_{IF}^s(nT_s)\right]\eta_0^*(nT_s-0.5T_c) \\ &+\left[S_{IF}^{a*}(nT_s-0.5T_c)+S_{IF}^{s*}(nT_s-0.5T_c)\right]\eta_0(nT_s) && \text{III} \\ &+\eta_0(nT_s)\eta_0^*(nT_s-0.5T_c) && \text{IV} \end{aligned} \tag{5}$$

As shown in (5), the right-hand side of the equation can be divided into four parts, identified by I–VI.

I: First part of the right-hand side of (5).

$$\begin{aligned} &S_{IF}^a(nT_s)\times S_{IF}^{a*}(nT_s-0.5T_c) \\ &= \sum_{i=1}^{M}\left\{\begin{array}{l} P_i^a D_i^a\left(nT_s-\tau_i^a\right)D_i^a\left(nT_s-\tau_i^a-0.5T_c\right)c_i\left(nT_s-\tau_i^a\right) \\ c_i\left(nT_s-\tau_i^a-0.5T_c\right)e^{j\pi(f_{IF}+f_{di}^a)T_c}\end{array}\right\} \\ &+\sum_{i=1}^{M}\sum_{\substack{q=1\\q\neq i}}^{M}\left\{\begin{array}{l}\sqrt{P_i^aP_q^a}D_i^a\left(nT_s-\tau_i^a\right)D_q^a\left(nT_s-\tau_q^a-0.5T_c\right)c_i\left(nT_s-\tau_i^a\right) \\ c_q\left(nT_s-\tau_q^a-0.5T_c\right)e^{j2\pi(f_{di}^a-f_{dq}^a)nT_s+j\pi(f_{IF}+f_{dq}^a)T_c+j(\varphi_i^a-\varphi_q^a)}\end{array}\right\} \\ &\approx \frac{1}{2}\sum_{i=1}^{M}P_i^a e^{j\pi f_{IF}T_c}+\sum_{i=1}^{M}\sum_{\substack{q=1\\q\neq i}}^{M}\left\{\begin{array}{l}\sqrt{P_i^aP_q^a}c_iD_i^a\left(nT_s-\tau_i^a\right)D_q^a\left(nT_s-\tau_q^a-0.5T_c\right) \\ c_i\left(nT_s-\tau_i^a\right)c_q\left(nT_s-\tau_q^a-0.5T_c\right) \\ e^{j2\pi(f_{di}^a-f_{dq}^a)nT_s+j\pi(f_{IF}+f_{dq}^a)T_c+j(\varphi_i^a-\varphi_q^a)}\end{array}\right\}\end{aligned} \tag{6}$$

Similarly, with (6) we can get $S_{IF}^s(nT_s)\times S_{IF}^{s*}(nT_s-0.5T_c)$ as follows:

$$\begin{aligned} &S_{IF}^s(nT_s)\times S_{IF}^{s*}(nT_s-0.5T_c) \\ &\approx \frac{1}{2}\sum_{i=1}^{M}P_i^s e^{j\pi f_{IF}T_c} \\ &+\sum_{i=1}^{M}\sum_{\substack{q=1\\q\neq i}}^{M}\left\{\begin{array}{l}\sqrt{P_i^sP_q^s}D_i^s\left(nT_s-\tau_i^s\right)D_q^s\left(nT_s-\tau_q^s-0.5T_c\right) \\ c_i\left(nT_s-\tau_i^s\right)c_q\left(nT_s-\tau_q^s-0.5T_c\right) \\ e^{j2\pi(f_{di}^s-f_{dq}^s)nT_s+j\pi(f_{IF}+f_{dq}^s)T_c+j(\varphi_i^s-\varphi_q^s)}\end{array}\right\}\end{aligned} \tag{7}$$

II: Second part of the right-hand side of (5):

$$\begin{aligned} &S_{IF}^a(nT_s)\times S_{IF}^{s*}(nT_s-0.5T_c) \\ &=\sum_{i=1}^{M}\sum_{q=1}^{M}\left\{\begin{array}{l}\sqrt{P_i^aP_q^s}D_i^a\left(nT_s-\tau_i^a\right)D_q^s\left(nT_s-\tau_q^s-0.5T_c\right) \\ c_i\left(nT_s-\tau_i^a\right)c_q\left(nT_s-\tau_q^s-0.5T_c\right) \\ e^{j2\pi(f_{di}^a-f_{dq}^s)nT_s+j\pi(f_{IF}+f_{dq}^s)T_c+j(\varphi_i^a-\varphi_q^s)}\end{array}\right\}\end{aligned} \tag{8}$$

Similarly, with (8) we can get $S_{IF}^s(nT_s)\times S_{IF}^{a*}(nT_s-0.5T_c)$ as follows:

$$\begin{aligned} &S_{IF}^s(nT_s)\times S_{IF}^{a*}(nT_s-0.5T_c) \\ &=\sum_{i=1}^{M}\sum_{q=1}^{M}\left\{\begin{array}{l}\sqrt{P_i^sP_q^a}D_i^s\left(nT_s-\tau_i^s\right)D_q^a\left(nT_s-\tau_q^a-0.5T_c\right) \\ c_i\left(nT_s-\tau_i^s\right)c_q\left(nT_s-\tau_q^a-0.5T_c\right) \\ e^{j2\pi(f_{di}^s-f_{dq}^a)nT_s+j\pi(f_{IF}+f_{dq}^a)T_c+j(\varphi_i^s-\varphi_q^a)}\end{array}\right\}\end{aligned} \tag{9}$$

III: Third part of the right-hand side of (5):

$$\left[S_{IF}^a(nT_s)+S_{IF}^s(nT_s)\right]\times\eta_0^*(nT_s-0.5T_c)\approx\eta_1(nT_s) \tag{10}$$

where $\eta_1(nT_s)$ is a circularly symmetric complex additive white Gaussian noise process. The distribution of $\eta_1(nT_s)$ can be written as

$$\eta_1(nT_s)\sim N\left(\begin{bmatrix}0\\0\end{bmatrix},\delta_0^2\left(\sum_{i=1}^{M}P_i^a+\sum_{q=1}^{M}P_q^s\right)\begin{bmatrix}1&0\\0&1\end{bmatrix}\right) \tag{11}$$

Similarly, with (10) we can get

$$\left[S_{\mathrm{IF}}^{\mathrm{a}*}(nT_{\mathrm{s}}-0.5T_{\mathrm{c}})+S_{\mathrm{IF}}^{\mathrm{s}*}(nT_{\mathrm{s}}-0.5T_{\mathrm{c}})\right]\times\eta_0(nT_{\mathrm{s}})$$

as follows:

$$\left[S_{\mathrm{IF}}^{\mathrm{a}*}(nT_{\mathrm{s}}-0.5T_{\mathrm{c}})+S_{\mathrm{IF}}^{\mathrm{s}*}(nT_{\mathrm{s}}-0.5T_{\mathrm{c}})\right]\times\eta_0(nT_{\mathrm{s}})\approx\eta_2(nT_{\mathrm{s}}) \tag{12}$$

where $\eta_2(nT_{\mathrm{s}})$ is a circularly symmetric complex additive white Gaussian noise process. The distribution of $\eta_2(nT_{\mathrm{s}})$ can be written as

$$\eta_2(nT_{\mathrm{s}})\sim N\left(\begin{bmatrix}0\\0\end{bmatrix},\delta_0^2\left(\sum_{i=1}^{M}P_i^{\mathrm{a}}+\sum_{q=1}^{M}P_q^{\mathrm{s}}\right)\begin{bmatrix}1&0\\0&1\end{bmatrix}\right) \tag{13}$$

VI: Fourth part of the right-hand side of (5):

$$\eta_0(nT_{\mathrm{s}})\eta_0^*(nT_{\mathrm{s}}-0.5T_{\mathrm{c}})\approx\eta_3(nT_{\mathrm{s}}) \tag{14}$$

where $\eta_3(nT_{\mathrm{s}})$ is a circularly symmetric complex additive white Gaussian noise process. The distribution of $\eta_3(nT_{\mathrm{s}})$ can be written as

$$\eta_3(nT_{\mathrm{s}})\sim N\left(\begin{bmatrix}0\\0\end{bmatrix},2\delta_0^4\begin{bmatrix}1&0\\0&1\end{bmatrix}\right) \tag{15}$$

According to previous assumptions, $\eta_0(nT_{\mathrm{s}})$ is complex additive white Gaussian noise with zero mean (Jafarnia-Jahromi et al. 2014). The noise component is assumed to be uncorrelated in the receiver operational bandwidth. Therefore, we can get the normal distribution characteristics of $\eta_3(nT_{\mathrm{s}})$, as is shown in (15).

Estimation of new noise level model

As discussed previously, $u[k,1]$ can directly reflect the signal components including both spoofing signals and the authentic signals, while for $p\geq 2$, the $u[k,p]$ directly reflects the noise level. The methodology to estimate the noise is the crucial part of spoofing detection. This section mainly provides an analysis of the new noise level model which is different from traditional definitions. We can estimate the noise level through the following equation:

$$\hat{\sigma}^2=\frac{1}{4086}\sum_{p=2}^{2044}\left|u[k,p]\right|^2=\frac{1}{2}\mathrm{var}\left[u[k,p]\right] \tag{16}$$

where $\mathrm{var}\left[u[k,p]\right]$ means taking the variance of $u[k,p]$. Then, we can get $\hat{\sigma}^2$, through analyzing each part of $u[k,p]$.

Here, we have an analysis of the variance of the first part of (5). We define two new variables

$$\psi_{\mathrm{aa}}[k]=\frac{1}{N}\sum_{n=(k-1)N+1}^{kN}S_{\mathrm{IF}}^{\mathrm{a}}(nT_{\mathrm{s}})\times S_{\mathrm{IF}}^{\mathrm{a}*}\left(nT_{\mathrm{s}}-\frac{p}{2}T_{\mathrm{c}}\right) \tag{17}$$

$$\psi_{\mathrm{ss}}[k]=\frac{1}{N}\sum_{n=(k-1)N+1}^{kN}S_{\mathrm{IF}}^{\mathrm{s}}(nT_{\mathrm{s}})\times S_{\mathrm{IF}}^{\mathrm{s}*}\left(nT_{\mathrm{s}}-\frac{p}{2}T_{\mathrm{c}}\right) \tag{18}$$

According to (6) and (17), the distribution of $\psi_{\mathrm{aa}}[k]$ can be written as

$$\psi_{\mathrm{aa}}[k]\sim N\left(\begin{bmatrix}0\\0\end{bmatrix},\sum_{i=1}^{M}\sum_{q=1}^{M}P_i^{\mathrm{a}}P_q^{\mathrm{a}}\begin{bmatrix}\delta^2&0\\0&\delta^2\end{bmatrix}\right) \tag{19}$$

According to (7) and (18), the distribution of $\psi_{\mathrm{ss}}[k]$ can be written as

$$\psi_{\mathrm{ss}}[k]\sim N\left(\begin{bmatrix}0\\0\end{bmatrix},\sum_{i=1}^{M}\sum_{q=1}^{M}P_i^{\mathrm{s}}P_q^{\mathrm{s}}\begin{bmatrix}\delta^2&0\\0&\delta^2\end{bmatrix}\right) \tag{20}$$

where δ^2 is a fixed value which is extracted to be $\delta^2\approx 0.00033$ (Jafarnia-Jahromi et al. 2012). As shown in (19) and (20), $\psi_{\mathrm{aa}}[k]$ depends on the power of authentic signals and $\psi_{\mathrm{ss}}[k]$ depends on the power of spoofing signals.

Then similarly with the analysis procedure of (17)–(20), we define another two new variables $\psi_{\mathrm{as}}[k]$ and $\psi_{\mathrm{sa}}[k]$

$$\psi_{\mathrm{as}}[k]=\frac{1}{N}\sum_{n=(k-1)N+1}^{kN}S_{\mathrm{IF}}^{\mathrm{a}}(nT_{\mathrm{s}})\times S_{\mathrm{IF}}^{\mathrm{s}*}\left(nT_{\mathrm{s}}-\frac{p}{2}T_{\mathrm{c}}\right) \tag{21}$$

$$\psi_{\mathrm{sa}}[k]=\frac{1}{N}\sum_{n=(k-1)N+1}^{kN}S_{\mathrm{IF}}^{\mathrm{s}}(nT_{\mathrm{s}})\times S_{\mathrm{IF}}^{\mathrm{a}*}\left(nT_{\mathrm{s}}-\frac{p}{2}T_{\mathrm{c}}\right) \tag{22}$$

According to (8) and (21), the distribution of $\psi_{\mathrm{as}}[k]$ can be written as

$$\psi_{\mathrm{as}}[k]\sim N\left(\begin{bmatrix}0\\0\end{bmatrix},\sum_{i=1}^{M}\sum_{q=1}^{M}P_i^{\mathrm{a}}P_q^{\mathrm{s}}\begin{bmatrix}\delta^2&0\\0&\delta^2\end{bmatrix}\right) \tag{23}$$

According to (9) and (22), the distribution of $\psi_{\mathrm{sa}}[k]$ can be written as

$$\psi_{\mathrm{sa}}[k]\sim N\left(\begin{bmatrix}0\\0\end{bmatrix},\sum_{i=1}^{M}\sum_{q=1}^{M}P_i^{\mathrm{s}}P_q^{\mathrm{a}}\begin{bmatrix}\delta^2&0\\0&\delta^2\end{bmatrix}\right) \tag{24}$$

Comparing (23) with (24), $\psi_{\mathrm{as}}[k]$ and $\psi_{\mathrm{sa}}[k]$ can be assumed to be equivalent. The characteristics of $\psi_{\mathrm{as}}[k]$ and $\psi_{\mathrm{sa}}[k]$ depend on the power of authentic signals and spoofing signals.

Based on the above discussions, $u[k,p](2\leq p\leq 2044)$ can be approximated as a complex Gaussian random variable with the following distribution:

$$u[k,p] \sim N\left(\begin{bmatrix} 0 \\ 0 \end{bmatrix}, \begin{bmatrix} \frac{2\delta_0^2}{N}\left(\sum_{i=1}^{M} P_i^{\mathrm{a}} + \sum_{q=1}^{M} P_q^{\mathrm{s}}\right) + \frac{2\delta_0^4}{N} \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \sum_{i=1}^{M}\sum_{q=1}^{M}\left(P_i^{\mathrm{a}}P_q^{\mathrm{a}} + P_i^{\mathrm{s}}P_q^{\mathrm{s}} + 2P_i^{\mathrm{a}}P_q^{\mathrm{s}}\right) \begin{bmatrix} \delta^2 & 0 \\ 0 & \delta^2 \end{bmatrix} \right) \tag{25}$$

Then, we can get $\hat{\sigma}^2$ as follows:

$$\hat{\sigma}^2 = \frac{N_0}{NT_{\mathrm{s}}}\left(\sum_{i=1}^{M} P_i^{\mathrm{a}} + \sum_{q=1}^{M} P_q^{\mathrm{s}} + \frac{N_0}{2T_{\mathrm{s}}}\right) + \sum_{i=1}^{M}\sum_{q=1}^{M}\left(P_i^{\mathrm{a}}P_q^{\mathrm{a}} + P_i^{\mathrm{s}}P_q^{\mathrm{s}} + 2P_i^{\mathrm{a}}P_q^{\mathrm{s}}\right)\delta^2 \tag{26}$$

where N_0 means the spectral density of the additive white Gaussian noise, which is assumed to be − 204 dBW-Hz. With this, we have derived the expression of the noise level model. $\hat{\sigma}^2$ can be considerably affected in the presence of spoofing signals. Since the power of authentic signals is kept within strict boundaries, $\hat{\sigma}^2$ mainly depends on the power of spoofing signals. The next section will provide a detailed analysis of the factors that influence $\hat{\sigma}^2$.

Effect analysis of spoofing attack on $2\hat{\sigma}^2$

The interference caused by the spoofing attack can elevate the noise floor of the receiver processing. The receiver noise floor model has been estimated in the previous section, and this section is aimed at the effect of $\hat{\sigma}^2$ imposed by spoofing attack. Here we take $2\hat{\sigma}^2$ as the estimation value of noise floor. Since there is no actual physical definition for $2\hat{\sigma}^2$, it is dimensionless. But in order to express its strength feature more intuitively, we take "X" and "dBX" as the units of $2\hat{\sigma}^2$. The transformation law between "X" and "dBX" is the same as the transformation between "W" and "dBW." ("W" means the power unit "Watt.")

$$10\,[\mathrm{X}] = 10\log_{10}(10) = 10\,\mathrm{dBX} \tag{27}$$

As shown is in (27), the conversion between "X" and "dBX" is similar to that between "W" and "dBW."

Figure 2 shows the average spoofing power for the case of 15 authentic PRNs and 15 spoofing PRNs versus the noise floor estimation values. The power of each authentic PRN (P_{au}) is − 157 dBW. The power of each spoofing PRN rises from − 180 to − 120 dBW. As shown in the figure, the noise floor stays at about − 306.5 dBX, when the average power of spoofing PRNs (P_{sp}) is lower than − 157 dBW. While with the increase in the average power of spoofing PRNs, the noise floor estimation value increases gradually.

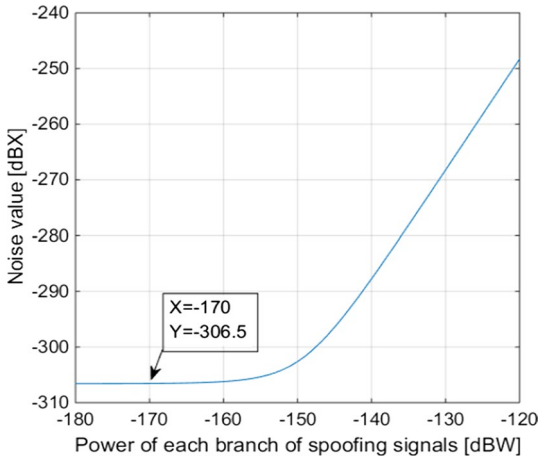

Fig. 2 Noise floor estimate versus P_{sp}

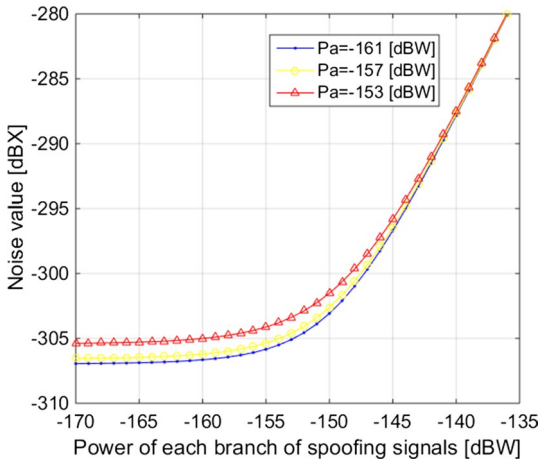

Fig. 3 Noise floor estimate for different values of P_{au}

Figure 3 shows the different cases of P_{au} (− 161, − 157 and − 153 dBW) versus the noise floor estimation values. From the three curves in Fig. 3, we can visually find that the stronger P_{au}, the higher will be the noise floor estimation level. But the distinctions among the three curves are not noticeable. That is because when P_{sp} is lower than P_{au}, the internal noise of the received signals plays a leading role, and when P_{sp} is higher than − 145 dBW, the spoofing signals play a leading role.

Figure 4 shows the noise floor estimation values for different choices of the number of available satellites. As P_{sp} is lower than − 160 dBW, the five curves are nearly the same. As P_{sp} keeps increasing, the differences between the five curves appear. But the variation tendency of the five curves is similar. In general, the number of available satellites for the user receiver is stable, and it can also be estimated from the almanac data stored in user receiver before.

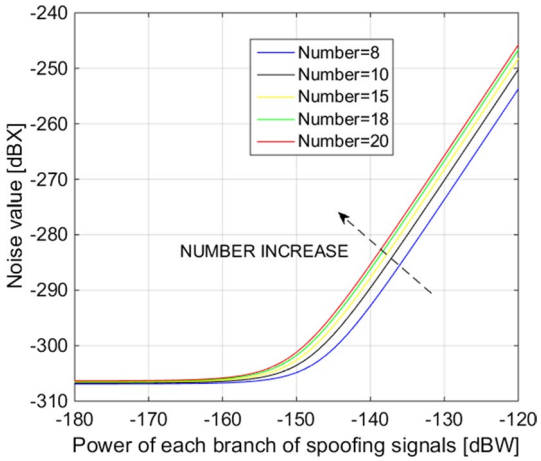

Fig. 4 Noise floor estimate for different choices of the number of satellites available

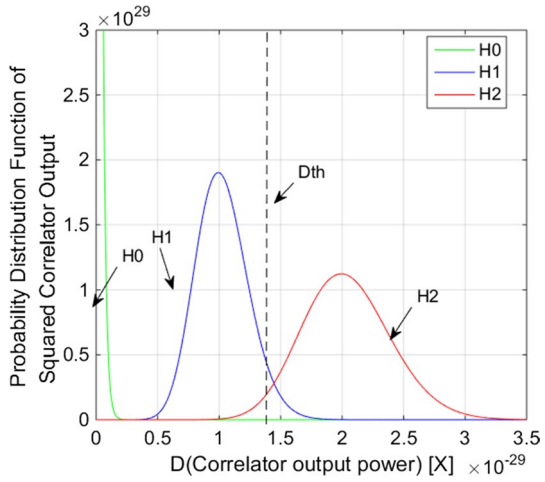

Fig. 5 Probability density distribution of D under ternary hypothesis test

A typical receiver is commonly equipped with an AGC system that changes the input amplifier gain in order to efficiently sample different signals with different levels. This AGC gain which is adjusted depending on the input signal power can be different in the presence and absence of spoofing signal. Then in order to measure real noise floor values, we must get the AGC gain values accurately which makes strict demands on the performance of GNSS receivers. Since the AGC gain similarly affects both signal and noise outputs, we can finish the spoofing detection task by compensating the effect of AGC, which will be discussed in detail in the next section.

Spoofing detection

The objective of analyzing the new noise floor model proposed in previous sections offers critical substance for the spoofing detection step. This section presents the implementation of spoofing detection. The invasion of a spoofing attack can considerably increase the observed noise floor of a GPS receiver. Here the correlation output value D is defined as follows:

$$D = u[k,1] \times u^*[k,1] \tag{28}$$

Then, the ternary hypothesis test is established as follows (Schonhoff and Giordano 2006):

H_0 (signals absent, $2\hat{\sigma}_0^2$)
H_1 (authentic signals present only, $2\hat{\sigma}_1^2$)
H_2 (both authentic and spoofing signals present, $2\hat{\sigma}_2^2$)

where $2\hat{\sigma}_0^2$, $2\hat{\sigma}_1^2$ and $2\hat{\sigma}_2^2$, respectively, denote the noise floor estimation under H_0, H_1 and H_2 hypothesis. In case that the number of authentic and spoofing PRN signals is 10, and the power of the spoofing signal is assumed to be − 157 dBW, i.e., the same with that of the authentic signal, the characteristic curves under the three Chi-square distributions below are presented in Fig. 5.

Under H_0, D can be written as central Chi-squared distributions with two degrees of freedom as follows:

$$p(D,\mathrm{H}_0) = \frac{1}{2\hat{\sigma}_0^2} \mathrm{e}^{-\frac{D}{2\hat{\sigma}_0^2}} \tag{29}$$

where $\hat{\sigma}_0^2$ means the estimated sampling variance of the correlation output value D, and $p(D,\mathrm{H}_0)$ denotes the probability distribution density under H_0 hypothesis, the characteristic curve is shown as a green line in Fig. 5.

Under H_1, D can be written as a non-central Chi-squared distribution with two degrees of freedom:

$$p(D,\mathrm{H}_1) = \frac{1}{2\hat{\sigma}_1^2} \mathrm{e}^{-\frac{D+a_1^2}{2\hat{\sigma}_1^2}} I_0\left(\frac{\sqrt{D}a_1}{\hat{\sigma}_1^2}\right) \tag{30}$$

$$a_1^2 = \frac{1}{4}\sum_{i=1}^{M} P_i^{\mathrm{a}} P_i^{\mathrm{a}} \tag{31}$$

where $\hat{\sigma}_1^2$ means the estimated sampling variance of the correlation output value D, $I_0(x)$ is the modified zero-order Bessel function of the first kind, and $p(D,\mathrm{H}_1)$ denotes the probability distribution density under H_1 hypothesis, the characteristic curve is shown as the blue line in Fig. 5.

Under H_2, D can be written as a non-central Chi-squared distribution with two degrees of freedom as:

$$p(D,\mathrm{H}_2) = \frac{1}{2\hat{\sigma}_0^2} \mathrm{e}^{-\frac{D+a_2^2}{2\hat{\sigma}_0^2}} I_0\left(\frac{\sqrt{D}a_2}{\hat{\sigma}_0^2}\right) \tag{32}$$

$$a_2^2 = \frac{1}{4}\sum_{i=1}^{M}\left(P_i^{\mathrm{a}}P_i^{\mathrm{a}} + P_i^{\mathrm{s}}P_i^{\mathrm{s}}\right) \tag{33}$$

where $\hat{\sigma}_2^2$ means the estimated sampling variance of the correlation output value D, and $p(D, \mathrm{H}_2)$ denotes the probability distribution density under H_2 hypothesis, the characteristic curve of which is shown as the red line in Fig. 5.

Here we focus on just spoofing detection, so we set the threshold D_{th} for the judgment of H_1 and H_2. If the correlator output value exceeds D_{th}, the spoofing attack may probably exist.

The probability of false alarm (P_{fa}) and the probability of detection (P_{d}) can be defined as:

$$P_{\mathrm{fa}} = \int_{D_{\mathrm{th}}}^{\infty} p(D, \mathrm{H}_1)\,\mathrm{d}D \tag{34}$$

$$P_{\mathrm{d}} = \int_{D_{\mathrm{th}}}^{\infty} p(D, \mathrm{H}_2)\,\mathrm{d}D \tag{35}$$

herein, when the receiver is equipped with an AGC system that changes the input amplifier gain in order to efficiently sample different signals with different power levels. In order to remove the effect of the AGC gain, we define a new variable TSNR as follows:

$$\mathrm{TSNR} = \frac{D}{2\hat{\sigma}^2} \tag{36}$$

As shown in (36), the definition of the new variable TSNR is similar to the traditional definition for SNR. Since the estimation noise value $2\hat{\sigma}^2$ and the correlation output value D are related to the spoofer's power advantage, TSNR will be affected as the spoofer's power changes. Combining (26), (28) and (36), we can get the variation tendency curve of TSNR versus P_{sp} as shown in Fig. 6.

Figure 6 shows the variation tendency of TSNR with the increase in P_{sp} ($P_{\mathrm{au}} = -157$ dBW, Number = 15). We can find that when P_{sp} is lower than -170 dBW, the value of TSNR keeps near 10 dB. When P_{sp} keeps increasing from -170 dBW, TSNR increases sharply. When P_{sp} is higher than -140 dBW, TSNR remains stable gradually with the value close to 26 dB.

Combining (34)–(36), we can get the receiver operating characteristic curve (ROC curve) for different values of P_{sp}, as shown in Fig. 7. It is observed that the detection performance of the receiver substantially gets better as P_{sp} increases. We can get the threshold $\mathrm{TSNR}_{\mathrm{th}} = 15.9$ dB for $P_{\mathrm{fa}} = 0.001\%$ as the probability of false alarm. Then, when P_{sp} is -151 dBW, P_{d} will be higher than 99.998%.

Simulation results

According to the published literature, it is quite difficult nowadays to get a complete platform for spoofing experiments tests, and it is illegal to spread spoofing signals outdoor. For the flexibility of GNSS software, it is practical to verify the proposed method with the help of GNSS software. The previous sections have shown specific decision processing of spoofing detection. This section presents experiments to testify the effectiveness of the new spoofing detection method based on GNSS software.

Jafarnia-Jahromi et al. (2014) proposed the SPA method for spoofing detection based on energy measurement. According to their Eq. (4), the periodic characteristic of $y_{\mathrm{ss}}^{\mathrm{cc}}(nT_{\mathrm{s}})$, i.e., the cross-correlation of different received PRN signals, depends on the frequency difference between two

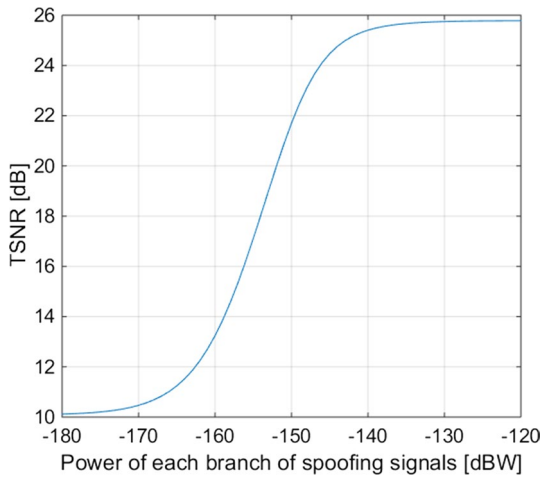

Fig. 6 Variation tendency of TSNR versus P_{sp}

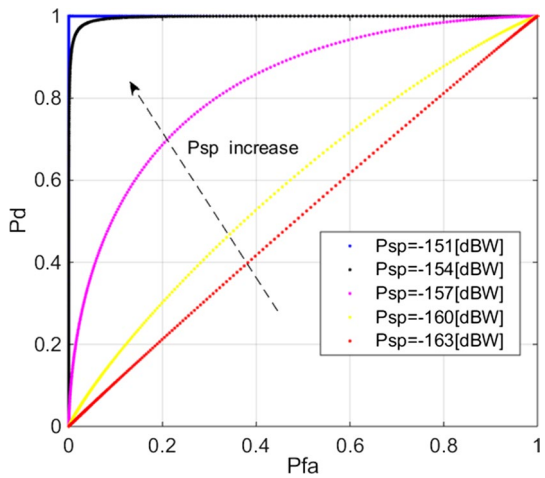

Fig. 7 ROC curve for different values of P_{sp}

PRNs. The frequency difference between two PRNs may change with time, so the periodic characteristic of $y_{ss}^{cc}(nT_s)$ changes with time too. That is to say that $y_{ss}^{cc}(nT_s)$ will not always get strengthened or weakened by the noise filtering process, which is likely to be the cause of test the statistics jumping violently. Based on the filtering theory of the SPA method, the energy of the signal is adequately extracted only when each Doppler frequency differences among the PRNs are n kHz, with n being an integer. However, we do not know sufficient information about code phase and Doppler frequency of the spoofing signals based on TEXBAT datasets (Humphreys et al. 2012). In that case, GNSS software provides a more practical and flexible simulation platform to verify the above predictions.

First simulation experiment

Applicability analysis of SPA method and TSEM method with different Doppler frequency choices.

$P_{au} = -157$ dBW; Number_au = Number_sp = 15; Time length: 6 s;
Time 0–5 s: Doppler frequencies of authentic signals and spoofing signals get a random variation every 1 s.
Time 5–6 s: In order to make sure that the Doppler frequency differences among different PRNs of authentic and spoofing signals are integer times of kHz, each Doppler frequency of the PRNs is reset to n kHz, and the integer n is randomly chosen within the range [− 5, 5].

In order to avoid the interaction between authentic signals and spoofing signals, the relative code phase difference between authentic signals and spoofing signals for the same PRN is limited to > 1.5 chips.

Figure 8 shows the SPA test statistics for simulated data in different situations such as spoofing absent (clean data), matched power 3 dB (the average power of spoofing is 3 dB higher than that of authentic signals), matched power 0.8 dB (the average power of spoofing is 0.8 dB higher than that of authentic signals), and overpowered (the average power of spoofing is 10 dB higher than that of authentic signals). It is observed that in the first 5 s, the test statistics stays at a low level, while after 5 s they undergo obvious uplift. The test statistics of the SPA method depend on the Doppler frequencies of spoofing signals and authentic signals, while under realistic environment, the Doppler frequencies are diversified. Based on the filtering theory of the SPA method, the energy of the signal is adequately extracted only when each Doppler frequency differences among the PRNs is n kHz, as shown at time 5–6 s. Now, therefore, we can justify that the SPA method has difficulties achieving practical performance levels.

Figure 9 shows the signals energy elevation based on TSEM method in different situations. As shown in the figure, the detection threshold $TSNR_{th} = 15.9$ dB is determined for the false alarm probability $P_{fa} = 0.001\%$. Even for the case when the average power of the spoofing signals is 0.8 dB higher than that of the authentic signals, the test statistics is 5 dB higher than in the case of when spoofing is absent. It is observed that the TSEM method can successfully detect the presence of spoofing signals.

Figure 10 shows the noise floor elevation in different situations. It is observed that the presence of spoofing signals slightly increases the receiver noise floor estimate. However, this slight increment might not provide considerable discrimination between authentic and spoofing signal sets.

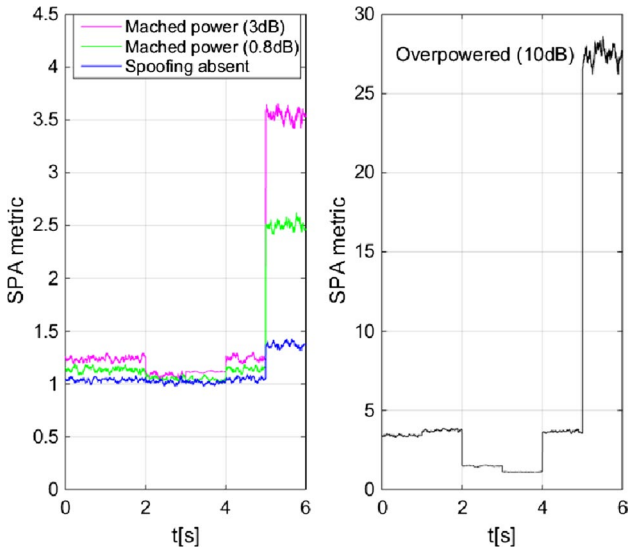

Fig. 8 Spoofing detection based on SPA method in different situations

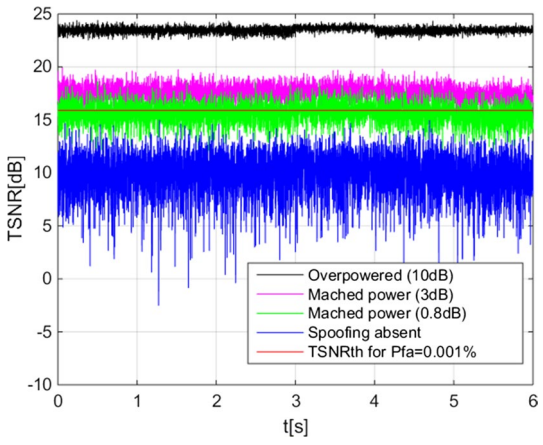

Fig. 9 Signals energy elevation based on TSEM method in different situations

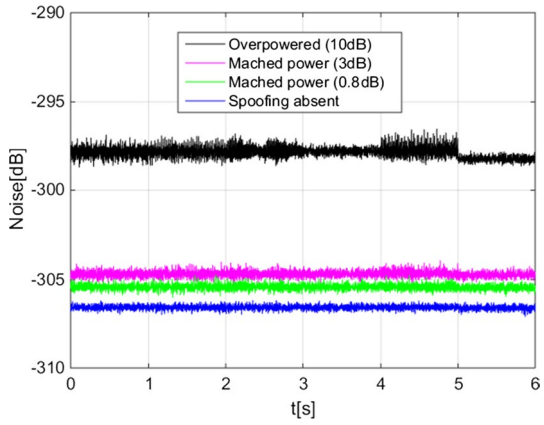

Fig. 10 Noise floor elevation based on TSEM method in different situations

Second simulation experiment

Code interval between spoofing PRNs and authentic PRNs is more than 1.5 chips

$P_{au} = P_{sp} = -157$ dBW; Number_au = Number_sp = 15; Time length: 1 s.

Code phase and Doppler frequency parameters: It is assumed that the relative Doppler frequency of spoofing signals and authentic signals is Δf and the carrier phases of the two signals are completely synchronous at the beginning. Also, the code phases of the two signals are kept at a half chip apart all the time.

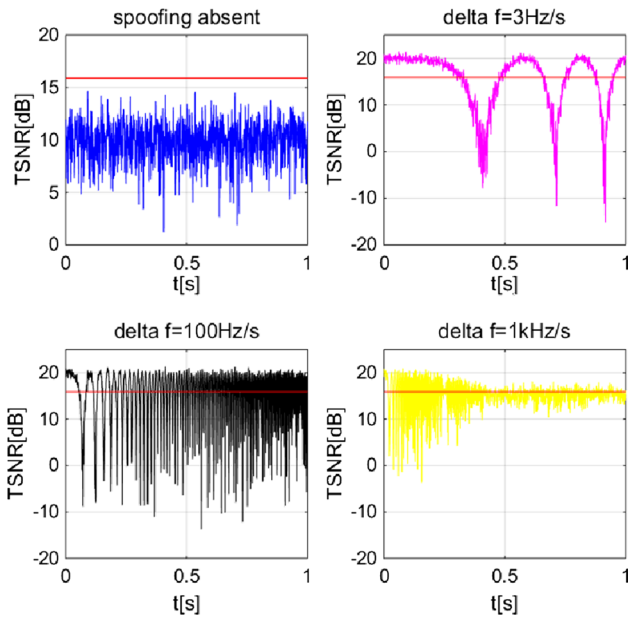

Fig. 11 Spoofing detection based on TSEM method in different situations

Figure 11 shows test statistics based on TSEM method. Four panels, respectively, illustrate four situations: spoofing absent and spoofing attack with $\Delta f = 3$ Hz/s, 100 Hz/s, and 1 kHz/s. We can know that the average power of the received signals without spoofing attack is about 10 dB, according to the upper left panel. As shown in the upper right panel, at the beginning the average power of the received signals is 20 dB which is much higher than $TSNR_{th}$, while it ranges from − 10 to 20 dB regularly. The lower left panel and the lower right panel illustrate similar characteristics. However, for the lower right panel, the test statistics tend to be relatively stable around 15 dB after 0.5 s. It is observed that when the Doppler frequency differences between spoofing signals and authentic signals are relatively small and the code phase differences are < 1.5 chips, the test statistics vary widely. When the Doppler frequency differences are in-phase, the test statistics get much higher than $TSNR_{th}$, which will improve the spoofing detection performance, while when the Doppler frequency differences are antiphase, the test statistics get much lower than $TSNR_{th}$, which will make the spoofing detection performance worse and even lose efficiency.

Just as stated above, the performance of the TSEM method will get worse when the code interval between authentic and PRNs is < 1.5 chips. The worst situation is that the spoofing signals and the authentic signals are antiphase with each other, the energy signals should be offset, and it is difficult for the receiver to detect the spoofing attack. This case is quite difficult to achieve for spoofer. On the one hand, the spoofer must know the motion state parameters of the receiver accurately and control various time delay precisely. On the other hand, the requirement of code phase difference and antiphase of Doppler frequency with the code interval < 1.5 chips will greatly limit the extension of spoofing, since the navigation results of a receiver depend on code phases and Doppler frequency. One common and practical spoofing pattern is: the spoofing power gradually increases and finally exceeds the authentic signal's power, and at the same time a higher power spoofing correlation peak is generated which gradually moves toward the authentic correlation peak and tries to grab the tracking point of the target receiver as shown in Fig. 12. When the receiver is under stable spoofed state, the TSEM method can detect

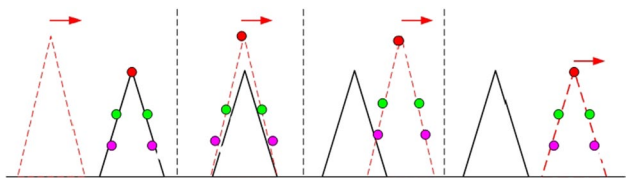

Fig. 12 Sliding spoofing attack on tracking phase of the user receiver

the existence of a spoofing attack effectively, since the code phases between the spoofing signals and authentic signals are more than 1.5 chips apart, in order to avoid interaction with each other.

Compared with spoofing attack, multipath signals may have some similar effects. Multipath signals are generally considered undesirable in GNSS because they destroy the correlation function shape used for time delay estimation. Multipath interference occurs when the user device receives reflected signals in addition to the direct line of sight (LOS) signal. These interference signals are generally reflected from the ground, buildings or trees in terrestrial navigation. In order to analyze the multipath effects on the TSEM method, the following simulation experiment is proposed.

Third simulation experiment

Analysis of multipath effects on TSEM method

$P_{au} = -157$ dBW; Number_au = 15; Time length: 1 s; Multipath number: 4.
Chip spacing separation from the authentic signals: 0.3 chip, 0.5 chip, 0.6 chip, 1.6 chips.
The power of multipath signals: − 160, − 162, − 164, − 161 dB.

It is assumed that the relative Doppler frequency of multipath signals and authentic signals is $\Delta f = 3$ Hz and the carrier phases of the two signals are completely synchronous at the beginning. In order to avoid the interaction between authentic signals and spoofing signals, the relative code phase difference between authentic signals and spoofing signals for the same PRN is limited to > 1.5 chips. In order to avoid the interaction between authentic signals and spoofing signals, the relative code phase difference between authentic signals and spoofing signals for the same PRN is limited to > 1.5 chips.

As shown in Fig. 13, the vast majority of the test statistics are under the threshold with multipath signals based on the TSEM method fluctuating more widely than the case without multipath signals shown in the upper left panel of Fig. 11. Generally, the multipath signals are from low-elevation angles of all available satellites, and the multipath signals are weaker than the authentic signals, while the spoofing signals are stronger than the authentic signals. The characteristics of multipath signals may change with time for a moving receiver, and it may make test statistics decrease or increase, which can lead to a false alarm or missed alarm. Since the time delay, attenuation factors, number of multipaths, and directions of multipaths are almost impossible to know, it is quite difficult to simulate the complex multipath environment completely. Therefore, it is not very easy to evaluate the bad effects of multipath signals on the detection performance of the TSEM method, and more research needs to be done.

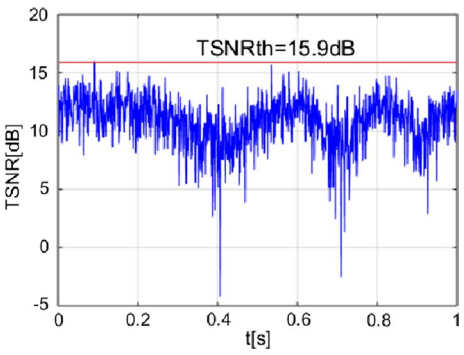

Fig. 13 Multipath effects on TSEM method

Nowadays, multipath remains a dominant source of ranging error in GNSS, and a large number of multipath suppression methods have been proposed. In order to enhance the robustness of the TSEM method, it is practical to take steps to reduce the bad effects of multipath signals on GNSS receivers. Since the multipath suppression problem will get more complex and difficult, once the receiver receives the multipath signal through the antenna, it is sensible to try to avoid the introduction of multipath signals. While choosing an open work area can effectively avoid multipath signals. Multipath suppression antenna will also do well against the introduction of multipath signals.

Fourth simulation experiment

TSEM method performance with spoofing power increasing

Time length: 14 s; $P_{au} = -157$ dBW; Number_au = Number_sp = 15;
Time 0–1 s: authentic signals present only;
Time 1 s: Spoofing attack starts, and the initial value of P_{sp} is − 172 dBW.
Time 1–14 s: P_{sp} is increasing from − 172 to − 133 dBW.
Power increasing speed of P_{sp} is 3 dB/s.

In order to avoid the interaction between authentic signals and spoofing signals, the relative code phase difference between authentic signals and spoofing signals for the same PRN is required to be > 1.5 chips.

Figures 14, 15, and 16 show the performance of the implemented spoofing detection method. Figure 14 shows that in the first 5 s ($P_{sp} \leq -160$ dBW), most of the TSNR values are below $TSNR_{th}$. As time increases, TSNR exceeds the $TSNR_{th}$ gradually. When P_{sp} is just slightly higher than P_{au}, the spoofing attack cannot cause obvious lifting to the noise floor estimation, since the signal components, both

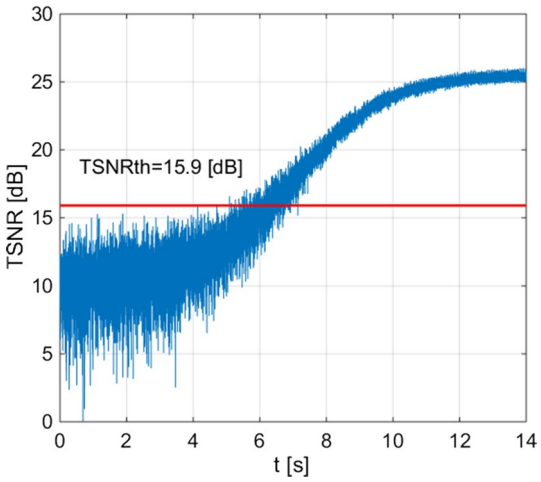

Fig. 14 Variation tendency of TSNR versus time (0–14 s)

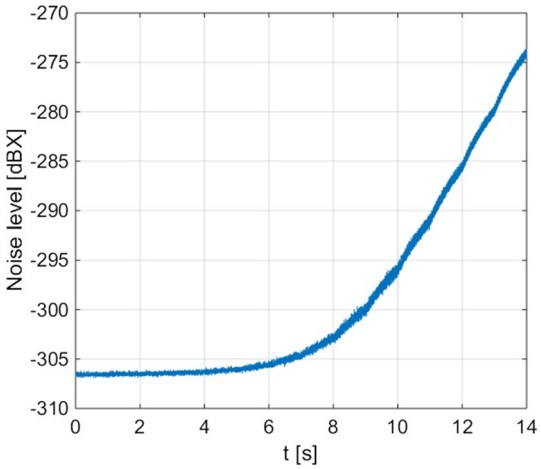

Fig. 15 Variation tendency of $2\hat{\sigma}^2$ versus time (0–14 s)

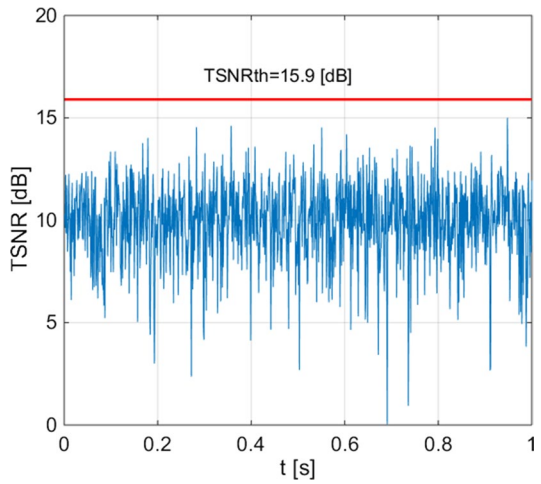

Fig. 16 Variation tendency of TSNR versus time (0–1 s)

authentic and spoofing signals, are far weaker than the noise component. In this case, it is quite difficult for the user receiver to realize the existence of a spoofing attack. The proposed TSEM method can help the user receiver detect the spoofing attack effectively. As shown in Fig. 14, after 7 s ($P_{sp} \geq -154$ dBW), most of the TSNR values are above $TSNR_{th}$. After about 12 s ($P_{sp} \geq -142$ dBW), TSNR keeps nearly constant.

When the AGC function is off, we can get the noise floor estimation $2\hat{\sigma}^2$ as shown in Fig. 15. In the first 5 s, $2\hat{\sigma}^2$ remains stable, while after 5 s, it starts to increase gradually. After 8 s, $2\hat{\sigma}^2$ increases sharply.

Figure 16 shows the variation of TSNR versus time in the first seconds (authentic signals present only). TSNR fluctuates near 10 dB, which is below $TSNR_{th}$. Therefore, the spoofing detection method proposed is useful for the case when only digital samples are available without despreading the IF signals.

Conclusions

The TSEM method which is based on measuring the energy of received signals can be used for GNSS spoofing detection. Through establishing new test quantities which can reflect the power of signal components and noise floor level, respectively, this spoofing detection system can work well when only digital samples are available, without knowing the code phase and Doppler frequency of each satellite and the AGC gain. The number of satellites available can be obtained from almanac data stored in the user receiver, as the prior information for the determination of detection threshold. In the end, the proper performance of this technique is verified through simulations based on GNSS software. The simulation results show that this method can work well even when the received signal strength of the spoofing and authentic signals are very close to each other when the spoofing signals are more than 1.5 chips apart from authentic signals. Also, the performance of spoofing detection gets better with the increase in spoofing signal strength.

However, there are yet no existing spoofing countermeasure techniques that can cope with all spoofing cases. Many countermeasures are confined to specific conditions. The nature of spoofing attack is that it represents not the real signals received from the satellites. The definition and classification of a spoofing attack are flexible rather than just a single fixed model taken from the existing literature. That is the reason why there are not yet existing spoofing countermeasure techniques that can cope with all spoofing cases. The spoofing detection method presented is based on the general assumption that the code phases of authentic signals and spoofing signals are independent of each other. Just as stated above, the TSEM method will meet some negative

factors for some special situations, such when the code phase differences between authentic signals and spoofing signals are < 1.5 chips, and the method needs to be adjusted or combined with other methods. But it is difficult to keep the code phases and Doppler frequencies accurate to meet the requirements for the spoofer to avoid being detected, which does well for the applicability of TSEM method. In addition, multipath signals can also negatively affect the robustness of the TSEM method, and further research is needed for multipath interference problems to improve its feasibility under complex multipath environment. Currently, it is practical and advisable for the TSEM method to be integrated with corresponding suppression technology to restrain or eliminate the multipath signals.

In summary, this spoofing detection system is easy to be applied on GNSS anti-spoofing receiver, with its characteristics being simple and effective. Especially for sophisticated spoofing signals transmitted by multi-antenna strategies for which many anti-spoofing countermeasures may lose efficacy, this method can work generally well, since it does not rely on the directions of received signals. But further developments are needed in order to produce a sufficiently reliable detection system for other spoofing cases such as under complex multipath conditions which have not been thoroughly evaluated in this paper.

Acknowledgements This work is financially supported by the National Natural Science Foundation of China (Nos. 41704034, 41631072 and 41504029). Thanks for the valuable comments and suggestions from the editorial office and the reviewers, which are quite helpful for us to improve its performance!

References

Akos D (2012) Who's afraid of the spoofer? GPS/GNSS spoofing detection via automatic gain control (AGC). Navigation 59(4):281–290

Bardout Y (2011) Authentication of GNSS position: an assessment of spoofing detection methods. In: Proceedings of ION GNSS 2011, Institute of Navigation, Portland, OR, USA, Sept 20–23, pp 436–446

Broumandan A, Jafarnia-Jahromi A, Dehghanian V, Nielsen J, Lachapelle G (2012) GNSS spoofing detection in handheld receivers based on signal spatial correlation. In: Proceedings of IEEE/ION PLANS 2012, Institute of Navigation, Myrtle Beach, SC, USA, Apr 24–26, pp 479–487

Broumandan A, Jafarnia-Jahromi A, Lachapelle G (2015) Spoofing detection, classification and cancelation (SDCC) receiver architecture for a moving GNSS receiver. GPS Solut 19(3):475–487

Dehghanian V, Nielsen J, Lachapelle G (2012) GNSS spoofing detection based on receiver C/No estimates. In: Proceedings of ION GNSS 2012, Institute of Navigation, Nashville, TN, USA, Sept 17–21, pp 2878–2884

Heng L, Work D, Gao G (2015) GPS signal authentication from cooperative peers. IEEE Trans Intell Transp Syst 16(4):1794–1805

Humphreys T (2013) Detection strategy for cryptographic GNSS anti-spoofing. IEEE Trans Aerosp Electron Syst 49(2):1073–1090

Humphreys T, Bhatti J, Shepard D, Wesson K (2012) The Texas spoofing test battery: toward a standard for evaluating GPS signal authentication techniques. In: Proceedings of ION GNSS 2012, Institute of Navigation, Nashville, TN, USA, Sept 17–21

Hwang P, McGraw G (2014) Receiver autonomous signal authentication (RASA) based on clock stability analysis. In: Proceedings of IEEE/ION PLANS 2014, Institute of Navigation, Monterey, CA, USA, May 5–8, pp 270–281

Jafarnia-Jahromi A, Broumandan A, Nielsen J, Lachapelle G (2012) GPS spoofer countermeasure effectiveness based on signal strength, noise power, and C/N0 measurements. Int J Satell Commun Netw 30(4):181–191

Jafarnia-Jahromi A, Daneshmand S, Broumandan A, Nielsen J, Lachapelle G (2013) PVT solution authentication based on monitoring the clock state for a moving GNSS receiver. In: European navigation conference (ENC) 2013, The European Group of Institutes of Navigation, Vienna, Austria, Apr 23–25, pp 1–11

Jafarnia-Jahromi A, Broumandan A, Nielsen J, Lachapelle G (2014) Pre-despreading authenticity verification for GPS L1 C/A signals. Navigation 61(1):1–11

Kerns A, Wesson K, Humphreys T (2014) A blueprint for civil GPS navigation message authentication. In: Proceedings of IEEE/ION PLANS 2014, Institute of Navigation, Monterey, CA, USA, May 5–8, pp 262–269

Khanafseh S, Roshan N, Langel S, Chan Fangcheng, Joerger M, Pervan B (2014) GPS spoofing detection using RAIM with INS coupling. In: Proceedings of IEEE/ION PLANS 2014, Institute of Navigation, Monterey, CA, USA, May 5–8, pp 1232–1239

Kuhn M (2005) An asymmetric security mechanism for navigation signals. In: Proceedings of international workshop on information hiding. Springer, Berlin, pp 239–252

Lee J, Kwon K, An D, Shim D (2015) GPS spoofing detection using accelerometers and performance analysis with probability of detection. Int J Control Autom Syst 13(4):951–959

O'Hanlon B, Psiaki M, Humphreys T, Bhatti J (2010) Real-time spoofing detection in a narrow-band civil GPS receiver. In: Proceedings of ION GNSS 2010, Institute of Navigation, Portland, OR, USA, Sept 21–24, pp 21–24

O'Hanlon B, Psiaki M, Humphreys T, Bhatti J (2012) Real-time spoofing detection using correlation between two civil GPS receiver. In: Proceedings of ION GNSS 2012, Institute of Navigation, Nashville, TN, USA, Sept 17–21, pp 3584–3590

O'Hanlon B, Psiaki M, Bhatti J, Shepard D, Humphreys T (2013) Real-time GPS spoofing detection via correlation of encrypted signals. Navigation 60(4):267–278

Psiaki M, Humphreys T (2016) GNSS spoofing and detection. Proc IEEE 104(6):1258–1270

Psiaki M, O'Hanlon B, Bhatti J, Shepard D, Humphreys T (2013) GPS spoofing detection via dual-receiver correlation of military signals. IEEE Trans Aerosp Electron Syst 49(4):2250–2267

Psiaki M, O'Hanlon B, Powel S, Bhatti J, Wesson D, Humphreys T (2014) GNSS spoofing detection using two-antenna differential carrier phase. In: Proceedings of ION GNSS + 2014, The Institute of Navigation, Tampa, FL, USA, Sept 8–12, pp 2776–2800

Schonhoff T, Giordano A (2006) Detection and estimation theory and its applications. Prentice Hall, Prentice

Shaofeng B, Yanfeng H, Bing J (2017) Research status and prospect of GNSS anti-spoofing technology. Sci Sin Inf 47(3):275–287

Shepard D, Humphreys T, Fansler A (2012) Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks. Int J Crit Infrastruct Prot 5(3):146–153

Volpe J (2001) Vulnerability assessment of the transportation infrastructure relying on the global positioning system. US Department of Transportation

Wesson K, Rothlisberger M, Humphreys T (2012) Practical cryptographic civil GPS signal authentication. Navigation 59(3):177–193

Yanfeng Hu received the B.S. degree in Radar Engineering and M.S. degree in Navigation, Guidance and Control from Naval University of Engineering, Wuhan, China, in 2012 and 2014, respectively. Now he is a doctoral student in the Department of Navigation Engineering, Naval University of Engineering. His main research includes: GNSS spoofing and anti-spoofing technology.

Shaofeng Bian received the B.S. degree in geodesy and M.S. degree in astronomical geodesy in Institute of Surveying and Mapping, the PLA Information Engineering University, Zhengzhou, China, in 1982 and 1985, respectively, and the Ph.D. degree from Wuhan Technical University of Surveying and Mapping in 1992. He was awarded an Alexander von Humboldt Research Fellowship, in 1996. He got founded by National Science Foundation for Distinguished Young Scholars, in 2001. He is a professor in the Department of Navigation Engineering, Naval University of Engineering.

Kejin Cao received the B.S. degree and M.S. degree in Naval Aeronautical Engineering Academy in 2000 and 2003, respectively, and the Ph.D. degree from Navy Electronic Engineering Institute in 2006. Currently, he is an Associate Professor in the Department of Navigation Engineering, Naval University of Engineering. His research interests include GNSS technology Loran-C technology.

Bing Ji received the M.S. degree from the PLA Information Engineering University in 2005 and Ph.D. degree from Naval University of Engineering in 2011. Currently, he is a Lecturer in the Department of Navigation Engineering, Naval University of Engineering. His research interests include GNSS technology and underwater.