Dear Reviewer,

- *Manuscript ID: sensors-387577*
- *Title: Spoofing Detection and Mitigation in a Multi-correlator GPS Receiver Based on the Maximum Likelihood Principle*
- *Authors: Yanbing Guo, Lingjuan Miao and Xi Zhang*

Thank you very much for your comments. We hope that the revised manuscript has made sufficient improvements over the previous version. The paper has been carefully revised according to all the comments. We add necessary explanations and highlight the changes in the revised paper. Furthermore, we reply to all the advice carefully in this letter.

Sincerely yours

Authors' Responses

In this review the authors address in detail all the comments raised with explanations and justifications in the cover letter. However, sometimes the clarification is not reflected enough in the manuscript, which still leaves some doubt in the reader.

Comment 1

- *Response to comment 1 – Reply:*
  The authors explain clearly their view in the response. Although I am not fully convinced, the explanation is consistent. However, the discussion about the type of attack (locked frequency) must be moved in the introduction, in order to clarify from the beginning the scope adopted for the proposed method. Furthermore, the (strong!) assumption about the high C/N0 ratio for using the 'tan' relationship must be clearly declared before the algorithm description.

Response to comment 1:

Thank you for your suggestions, which are very helpful to better illustrate the application of the proposed method. According to your suggestions, the discussion about the type of attack (locked frequency) is included in the introduction:

"Based on the discussions above, the spoofing mitigation needs to be further researched in anti-spoofing. Multipath and spoofing share the similarity that they

distort the correlation peaks of the composite signals. In particular, if the carrier frequency of the counterfeit signal deviates from that of its corresponding authentic signal, the distortion of the correlation peak of the composite signal will be serious. Instead, if the carrier frequency of the counterfeit signal is consistent with that of its corresponding authentic signal, the correlation peak of the composite signal of spoofing will be similar to that of multipath, which is the most difficult situation to detect and handle. Hence, the carrier frequencies of the counterfeit signal and its corresponding authentic signal are set to be the same (frequency lock mode) [19]. As a result, multipath mitigation approaches can be applied to anti-spoofing [20]."

At the same time, the description of locked frequency at the beginning of Section IV is retained in order to re-emphasize this situation and to explain its feasibility.

Besides, the assumption about the high C/N_0 is clearly declared before the formula $\tan\left(\hat{\phi}\right)=\hat{y}/\hat{x}$ to help readers understand the scope applied for the 'tan' relationship:

"**Step 4.** Determine the carrier phase of the counterfeit signal.

In the process of determining the time delay and amplitude of the counterfeit signal, the calculations of $\hat{x}$ and $\hat{y}$ are involved in different cases. It should be pointed out that the C/N_0 of the authentic signals used in the experiments are relatively high. Correspondingly, the counterfeit signals whose power is slightly higher than that of their corresponding authentic signals also have relatively high C/N_0. Therefore, based on $\tan\left(\hat{\phi}\right)=\hat{y}/\hat{x}$, the estimated carrier phase of the counterfeit signal can be obtained in three cases. If $\hat{x}>0$, $\hat{\phi}=\arctan\left(\hat{y}/\hat{x}\right)$. If $\hat{x}<0$, $\hat{\phi}=\pi+\arctan\left(\hat{y}/\hat{x}\right)$. If $\hat{x}=0$, $\hat{\phi}=\mathrm{sgn}\left(\hat{y}\right)\pi/2$."

Comment 2

✧ *Response to comment 3 – Reply:*

The provided explanation has not been included in the manuscript: it should be at the beginning of section 3 for clarity.

Response to comment 2:

Thank you for your suggestions. The explanation about the number of counterfeit signals is added at the beginning of Section III:

"where A_0 is the known amplitude of the authentic signal, $D(\cdot)$ is the navigation data bit, $c(\cdot)$ is the CA code, N is the number of counterfeit signals in the current channel, $n=0,1,2,\cdots,N$, $v_{\mathrm{i}}(t)$ and $v_{\mathrm{q}}(t)$ denote the noises in the I and Q branches, respectively. $a_n(t)$, $\tau_n(t)$, $\phi_n(t)$ are the amplification coefficient of the amplitude, code delay (time delay) and carrier phase corresponding to the *n*-th signal, respectively. If $n=0$, they correspond to the authentic signal and

$a_0(t)=1,\quad \tau_0(t)=0,\quad \phi_0(t)=0$. Otherwise, they correspond to the counterfeit signals and $a_n(t)\geq\sqrt{1.1}$. In reality, the repeater delays and amplifies the authentic signal, and then rebroadcasts it. This principle determines that there is usually only one counterfeit signal corresponding to each satellite, namely, $N=1$. Although the counterfeit signals for spoofing can be ahead of the authentic signal, we assume $\tau_n(t)\geq 0$ by symmetry in order to facilitate the discussion."

Comment 3

✧ *Response to comment 4 – Reply:*

It is my opinion that also N does not comply with your assumption, not only \tau_n.

Response to comment 3:

Thank you for your comment. As you said, not only τ_n but also N does not comply with our assumption.

Since the value of N has been explained before, there is no need to assume that the value of N is known again. The original assumption is revised as follows:

"It can be assumed that τ_n is known to facilitate the estimation of signal parameters. In this case, only linear problems need to be solved (Actually, τ_n can hardly be consistent with our assumption. In this case, some additional strategies are needed to estimate τ_n. See Step 3 in Section IV for more details). The probability distribution function (PDF) of $\boldsymbol{I}_\Sigma$ given $\boldsymbol{X}_\Sigma$ can be expressed as

$$f\left(\boldsymbol{I}_\Sigma \mid \boldsymbol{X}_\Sigma\right)=\frac{1}{\left(\sqrt{2\pi}\right)^{M+1}\det\left(\boldsymbol{P}_\Sigma\right)^{1/2}}\exp\left\{-\frac{1}{2}\left[\boldsymbol{I}_\Sigma-\boldsymbol{G}_\Sigma\boldsymbol{X}_\Sigma\right]^T\boldsymbol{P}_\Sigma^{-1}\left[\boldsymbol{I}_\Sigma-\boldsymbol{G}_\Sigma\boldsymbol{X}_\Sigma\right]\right\}." \quad (16)$$

Comment 4

✧ *Response to comment 6 – Reply:*

✧ *The provided explanation has not been included in the manuscript: it should be for clarity.*

Response to comment 4:

Thank you for your suggestions. We sincerely apologize for the missing explanations in our paper. Since A_0 is related to C/N_0, a supplement to the calculation of C/N_0 and A_0 is first included in the revised manuscript:

"**Step 1.** Determine whether the signal amplitude of the *n*-th correlator is valid.

According to equations (20) and (21), the estimated x_n and y_n are obtained as $\hat{x}_n$ and $\hat{y}_n$ and $\hat{A}_n=\sqrt{\hat{x}_n^2+\hat{y}_n^2}$ denotes the estimate of $A_n=a_nA_0$. In order to facilitate the discussion, $\hat{A}_n$ is termed as the signal amplitude of the *n*-th correlator.

We choose the value of threshold A based on the carrier-to-noise ratio C/N_0 of the authentic signal. That is, the value of A is set according to A_0, which can be obtained from the stimulation of the authentic signal to the first correlator based on the assumption that the target receiver locks authentic signals in advance. If $\hat{A}_n > A$, $\hat{A}_n$ is valid. Otherwise, $\hat{A}_n$ is invalid."

Then the identification of the authentic signal is further explained in the revised manuscript:

"**Step 5.** Remove the counterfeit signal.

After detecting the time delay, amplitude and carrier phase of the counterfeit signal, the counterfeit signal is confirmed to have a short delay. The opposite counterfeit signal is added to the composite signal to restore the authentic signal. It is worth noting that the assumption of locking the authentic signal in advance can prevent us from mistakenly removing the authentic signal."

Finally, the setting of A is explained in the first paragraph of Section 5.2: "In addition, we let $A = 0.2A_0$ empirically."

We sincerely hope the added explanations can meet your requirements, and we should thank you again for the suggestions.

Comment 5

✧ *Overall, I remain highly doubtful about the effectiveness of the method in more realistic situations than in lab simulations; in particular, my major concern is the behavior of the algorithm when the assumptions are not met. I'd suggest the authors to try to elaborate on the boundaries of the scope of their algorithm and to discuss how to manage the out-of-scope situations.*

Response to comment 5:

Thank you for your suggestions. We sincerely apologize for the confusions. Here we try to further explain the application scope of our algorithm and discuss how we manage the out-of-scope situations. Besides the assumption that the target receiver has locked authentic signals before spoofing is applied, our algorithm is aimed at frequency lock mode. Corresponding methods in the presence of unlocked frequency are added in the revised manuscript:

"The whole process of detecting and removing the counterfeit signal is elaborated above. Due to the complexity and variability of deliberate interferences, it is very difficult for one single anti-spoofing method to properly handle all kinds of spoofing. For example, the anti-spoofing method based on the multi-correlator structure can help the tracking receiver to keep the authentic signal locked. However, if there already exists spoofing during acquisition, this method will be incapable of

distinguishing between the authentic and counterfeit signals of the receiver. Therefore, multiple anti-spoofing methods should be adopted in the receiver simultaneously [18]. For instance, if the counterfeit signal corresponding to each satellite comes from a single interference source, the antenna can be moved along any small trajectory. In this case, the relative motion between the receiver and the repeater makes the variation of the carrier frequency of each counterfeit signal exactly the same. If the multi-correlator structure can detect the spoofing at the initial tracking stage, this method can be introduced to help the receiver determine whether the locked signal is the authentic signal. If spoofing with unlocked carrier frequency succeeds in spoofing the target receiver, significant abnormalities in the outputs of phase discriminators will be inevitable [19]. In this case, this method can also be introduced to help the receiver determine whether it is necessary to enter the reacquisition stage (If the carrier frequency difference between the counterfeit signal and its corresponding authentic signal increases to a relatively large value, two distinct correlation peaks will appear at the reacquisition stage. That is, the spoofing degenerates into the simplistic form). In addition, other common anti-spoofing methods can also be used on the receiver to detect the simplistic spoofing earlier or more conveniently and ensure the correctness of the positioning results."

We sincerely hope that the supplementary information can meet your requirements, and we thank you again for the suggestions to help us improve the manuscript.

Thank you very much for your valuable comments and suggestions. Again, we appreciate the reviewer for your time and effort in reviewing this paper. Thank you very much! If you have further questions, please feel free to let us know.