Received: 16 July 2021 | Revised: 25 February 2022 | Accepted: 28 April 2022

DOI: 10.33012/navi.534

ORIGINAL ARTICLE

Developing a Spoofer Error Envelope for Tracking GNSS Signals

Tobias Bamberg[1,2] | **Andriy Konovaltsev**[1] | **Michael Meurer**[1,2]

[1] Institute of Communications and Navigation, German Aerospace Center (DLR), Oberpfaffenhofen, Germany

[2] Chair of Navigation, RWTH Aachen University, Aachen, Germany

Correspondence
Tobias Bamberg
German Aerospace Center (DLR)
Muenchner Str. 20
82234 Wessling
Email: tobias.bamberg@dlr.de

Abstract

Global navigation satellite systems (GNSSs) are the most significant service for global positioning and timing. The high relevance and wide spread of these systems contrast with the risk for interference or even manipulations of GNSS signals. One specific threat is GNSS spoofing. A spoofer counterfeits satellite signals to mislead the receiver to an erring position/time estimation. The technological progress enabling affordable and easy-to-use spoofer hardware further increases the relevance of this threat. To maintain the integrity of the position/time information, it is mandatory to be able to assess the errors induced by spoofing. The paper at hand derives a bound of the code tracking bias in relevant spoofing scenarios extending the well-known Multipath Error Envelope. These new bounds can be used as a tool to estimate the position/time error, especially but not exclusively for receivers that are collateral damage of a spoofing attack.

Keywords

bounds, GNSS, Multipath Error Envelope, spoofing

1 | INTRODUCTION

Global navigation satellite systems (GNSSs) are widely used for positioning and timing. These systems are not only used as a navigation aid by land, air, and water vessels, but also by critical infrastructure elements as well as further automated and autonomous processes. The increasing number of private and commercial unmanned aerial vehicles (UAVs) and the upcoming of autonomous driving cars will further increase the number of systems relying on GNSSs. This results in significant economical, safety, and security risks associated with possible GNSS service disruptions caused by radio frequency interference (RFI) on navigation signals.

One specific type of such interference is spoofing: A spoofer transmits GNSS-like signals to affect the position, velocity, and time (PVT) solution of a GNSS receiver. In contrast to jamming, where the reception of the navigation signals is restrained or even blocked and the availability of the receiver's PVT solution is compromised, a spoofer attack aims at manipulating the PVT solution that is deceived by the counterfeit signals. A user affected by spoofing may not even realize that something is wrong, which compromises the integrity of GNSS positioning and timing services. The spoofing effect observed in the user receiver highly depends on the type of the spoofing attack (Humphreys et al., 2008).

This aspect is addressed in Fernández-Hernández et al. (2019), Günther (2014), and Humphreys et al. (2008), in which the possible types of spoofing are identified. One of the most general classifications of spoofing attacks is provided by Humphreys et al. (2008) from the perspective of the technical realization where three categories are proposed: simplistic, intermediate, and sophisticated spoofing.

Simplified, the simplistic attack is an unsynchronized spoofing attack, for example, by radiating GNSS signals produced by a suitable signal generator with the counterfeit signals not necessarily well-aligned with the corresponding authentic signals. Intermediate spoofing synchronizes each spoofing signal to the authentic one. However, in this category, the synchronization is assumed to be limited to the phase of the spreading code (i.e., of PRN code) and carrier Doppler. The most sophisticated realizations of spoofing falling into the last category are supposed to additionally exploit carrier-phase synchronicity and, possibly, multiple transmitters enabling different directions-of-arrival of the counterfeit signals in order to deceive a target receiver. Recently, Fernández-Hernández et al. (2019) suggested a new classification accounting for the operational aspects of spoofing mitigation with seven categories ranging from S1 to S7. In addition to the technical complexity, these categories also account for the intention of the spoofing if it is targeted or occurs as collateral damage.

From the point of view of the integrity of GNSS services, the most dangerous are scenarios in which the spoofer attempts to imperceptibly substitute the authentic satellite signals with their counterfeit copies so that the signal tracking process in the target receiver is least distorted. Such scenarios can be realized, for example, by using the spoofers of the intermediate or sophisticated types discussed above. In the initial phase of such a spoofing attack, each affected satellite channel would track the authentic signal but encounter a mixture of the authentic and counterfeit signals. The spoofer aims at overpowering the authentic signals without being recognized by the user and pulls the satellite channel away from the authentic signal. At the end of this phase, the stronger spoofing signal becomes the only signal being tracked (if we ignore the multipath-like effect of the still present authentic signal).

Being aware of this mechanism of a spoofing attack, the question arises: Is it possible to assess the effect of spoofing on the tracking process of the authentic signal? Such an assessment is not only beneficial for improving and developing receiver systems, but also for the development of new signal structures for future GNSSs that are more resilient against spoofing. It can be helpful to detect spoofing signals and mitigate their effects by configuring the tracking loop parameters, as well as developing integrity monitors. This is also a very interesting question from the point of view of assessing the collateral damage occurring at non-targeted GNSS receivers (e.g., in the case of using spoofing for taking control of an illegally used drone autonomously flying with GNSS navigation and preserving, at the same time, the correct operation of GNSS services for other users).

One of the most practical approaches to address the question is to apply the concept of an error envelope, bounding the maximum bias of the PRN-code phase tracking error. This concept has already been applied to the case of multipath propagation where a Multipath Error Envelope (MEE) is widely used (Teunissen & Montenbruck, 2017). Indeed, on the signal level, the spoofing signal is comparable to a multipath signal: Both are time-shifted replicas of the authentic/line-of-sight (LOS) satellite signal. Van Nee (1992) derived the MEE for the GPS L1 C/A signal, giving an overbound of the tracking error in the presence of a multipath signal.

Since then, the method was further developed to be more accurate (Braasch, 1997) and to cover other (newer) GNSS signals (Irsigler et al., 2004). However, the spoofing signal corresponds to a more generic case. Unlike the multipath signal, it can be received earlier than the authentic signal and its power can be higher. Taking into account that the MEE is limited to multipath signals which have less signal power than the corresponding LOS signals, the paper at hand will address this limitation by extending the concept of the Multipath Error Envelope for signals that can be stronger than the LOS signal: Spoofing signals. The correspondingly extended error envelope will be called the Spoofing Error Envelope (SEE).

The SEE will help to understand the basic mechanisms of how a spoofing signal affects satellite tracking in a classical GNSS receiver. It gives a sense of the expected (initial) tracking error after the spoofer is enabled. The SEE lays the foundation for further research and can be used to explain and predict simulated results (e.g., Bamberg et al. [2018]). The next section gives an overview over the assumptions made while deriving the SEE.

2 | SCENARIO DEFINITION AND ASSUMPTIONS

2.1 | Receiver

In a GNSS receiver, the processing of a satellite signal can be subdivided into two states: The acquisition state and the tracking state. The acquisition state is only used to acquire new satellite signals and to reacquire a signal that was lost in the tracking process. In order to ensure that all satellites are in the acquisition state, a spoofer would either need to jam the satellite signals before spoofing or be active before the receiver is switched on. The latter option is usually beyond the control of the spoofer. Jamming all satellites, on the other hand, is relatively easy to detect (e.g., by observing the automatic gain control level [Akos, 2012]) and the disruption of the service warns the user that something is wrong. In contrast, a receiver staying in the tracking state does not give obvious signs indicating a spoofing attack. It is, therefore, the more critical state. This paper assumes that the receiver tracks the authentic satellite signal before and stays in the tracking state when a spoofing signal is encountered.

In the tracking state, the tracking bias depends on the implemented tracking architecture. The classical and still widespread architecture to track a satellite signal is the delay lock loop (DLL). The DLL is fed by a discriminator indicating the residual tracking error. Different discriminators can be used (Kaplan & Hegarty, 2005). In order to define a bound, it is inevitable to restrict the type of architecture. Due to its wide spread, we assume a receiver using a DLL with an early-late discriminator (Kaplan & Hegarty, 2005). To this day, many GNSS receivers still highly rely on the GPS L1 C/A signal. Therefore, we will focus our research on the GPS L1 C/A signal. The method introduced in this paper can easily be extended to other signals and discriminators.

Last but not least, we assume that the receiver does not implement a dedicated approach to mitigate the spoofing signal. This assumption is justified by two facts. First, it is reasonable to expect that such an approach reduces the tracking bias. However, this paper aims to define a worst-case bound, which still holds. Second, most of the on-shelf GNSS receivers do not mitigate spoofing signals. Considering, for example, civil aviation. A receiver used in this field must fulfill the Minimal Operational Performance Standards (MOPS) as defined by RTCA SC-159 (2019).

For now, this standard does not include any methods to mitigate spoofing. A receiver using an approach to mitigate spoofing signals would probably even violate the standard.

2.2 | Scenario

For our analysis, we assume that the delay between the spoofing and the authentic signal remains constant. This is, for example, given when the spoofer generates signals faking a position with a constant offset to the real position (and a constant clock offset). A movement of the individual components (spoofer, receiver, satellites) is uncritical, as long as the spoofer accounts for the corresponding movement.

Naturally, in this scenario, a relative Doppler between the authentic and the spoofing signal is about zero to match the movement of the signal delay with the signal Doppler. However, a spoofer can generate counterfeit signals with an arbitrary (relative) Doppler. Therefore, we account for both cases: In the derivation of the bounds of the tracking bias, we assume no relative Doppler, whereas Section 6 discusses the effect of a relative Doppler on the derived bound.

2.3 | Summary

Summed up, we identified four assumptions which must hold in order to define a worst-case tracking bias:

1. The observed receiver is in and stays in its tracking state when the spoofing signal is encountered.
2. The GPS L1 C/A code signal is tracked and a classical early-late discriminator is used.
3. The observed receiver does not apply any approach to mitigate spoofing signals.
4. The delay between the spoofing and the authentic signal stays approximately constant (over the period under observation).

These assumptions should not be seen as limitations, rather they lay the foundation for further research. There are many relevant scenarios in which these assumptions are fulfilled. If we consider, for example, a spoofer aiming to deceive its victim unperceived, the spoofer must not use high power. High-power GNSS signals will knock out a receiver forcing it to go into its acquisition state. Therefore, such a spoofer transmits signals that drive the tracking loops of a victim receiver slowly from the authentic to the spoofing signal. To do this, the spoofer needs to be synchronized to the authentic signal at the receiving antenna of the victim. If the spoofer transmits its signals over the air, most static or slowly moving receivers, which use a classical early-late discriminator, fulfill the four assumptions.

2.4 | Spoofer

Regarding the spoofer, these assumptions can be fulfilled by an intermediate or sophisticated spoofer that is synchronized to the authentic signals. According to the classification of Fernández-Hernández et al. (2019), all categories except S2 and S3 can (theoretically) fulfill the assumptions.

3 | SIGNAL TRACKING AND THE MULTIPATH ERROR ENVELOPE

Prior to defining the Spoofer Error Envelope (SEE), some relevant aspects of GNSS signal processing are discussed in this section. Also, the Multipath Error Envelope that serves as a starting point for this research is shortly reviewed.

In order to estimate the user's position, a GNSS receiver calculates pseudoranges for each satellite. A pseudorange includes the distance and the clock offset between the satellite and the receiver. To calculate the pseudorange, a precise receiving time of the incoming satellite signal is obligatory. This time is obtained by correlating the incoming signal with a time-shifted local replica of the known PRN code of the satellite. In addition, the incoming signal is correlated with a Doppler-shifted carrier to account for the relative velocity between the satellite and the receiver. The two-dimensional correlation function is called the Ambiguity Function (Presti & Motella, 2010). The highest peak of this ambiguity function indicates the best match of the local with the satellite signals. In the acquisition state, the receiver aims to find a coarse match by considering a large number of time-shifts and Doppler frequencies. After the acquisition, a conventional receiver computes only a small number of correlations (to save computational power) to track the peak of the ambiguity function. This process is referred to as tracking.

As stated in Section 2, we assume that the code tracking is performed by a DLL using a code discriminator. The output of the discriminator that is computed using the correlation results has to be proportional to the misalignment between the local reference and the received PRN code. In the presence of two time-shifted signals with the same PRN code (e.g., a satellite signal and a multipath), the discriminator function (also called S-curve) is distorted. This distortion drives the DLL to track an offset relative to the satellite signal.

This section starts with a mathematical description of the ambiguity function (Section 3.1) and the discriminator function (Section 3.2) in a degraded scenario. Section 3.3 describes the effect of the discriminator function on the tracking. The last subsection (Section 3.4) is a short recap of the Multipath Error Envelope.

3.1 | Ambiguity Function in the Presence of an Additional Signal

An approximated ambiguity function in the absence of noise for a single satellite signal is given as (Presti & Motella, 2010):

$$S(\tau, f_{\mathrm{o}}) = \frac{A}{2} e^{-\mathrm{j}\varphi} R(\tau) \operatorname{sinc}(f_{\mathrm{o}} T_c) \tag{1}$$

where φ describes the (initial) offset of the phase, τ describes the offset of the code (lag value) in units of PRN chips, and f_{o} describes the offset of the Doppler frequency between the local replica and the incoming satellite signal. The parameter A is the amplitude of the satellite signal and T_c is the (coherent) integration time of the correlation. The function $R(.)$ represents the normalized autocorrelation function of the PRN code and $\operatorname{sinc}(.)$ represents the normalized sinc-function defined as $\operatorname{sinc}(x) = \frac{\sin(\pi x)}{\pi x}$.

Due to the linearity of the correlation process, the ambiguity function of the superposition of a satellite and one additional signal (with the same PRN) can be described as:

$$\begin{aligned} S_{\Sigma}(\tau, f_{\mathrm{o}}) \\ &= \frac{A_{\mathrm{sat}}}{2} e^{-\mathrm{j}\varphi_{\mathrm{sat}}} R(\tau) \operatorname{sinc}(f_{\mathrm{o}} T_c) \\ &\quad + \frac{A_{\mathrm{add}}}{2} e^{-\mathrm{j}\varphi_{\mathrm{add}}} R(\tau - d_{\mathrm{sa}}) \operatorname{sinc}((f_{\mathrm{o}} - f_{\mathrm{sa}}) T_c) \end{aligned} \tag{2}$$

$$\begin{aligned} &= \frac{A_{\mathrm{sat}}}{2} e^{-\mathrm{j}\varphi_{\mathrm{sat}}} \operatorname{sinc}(f_{\mathrm{o}} T_c) \\ &\left[R(\tau) + \alpha e^{-\mathrm{j}\Theta} R(\tau - d_{\mathrm{sa}}) \frac{\operatorname{sinc}((f_{\mathrm{o}} - f_{\mathrm{sa}}) T_c)}{\operatorname{sinc}(f_{\mathrm{o}} T_c)} \right] \end{aligned} \tag{3}$$

where d_{sa} is the relative signal delay (in units of chips) and f_{sa} the relative frequency offset between the satellite and the additional signal. The subscripts *sat* and *add* indicate that the parameter refers to the satellite and the additional signal, respectively.

Furthermore, we define two parameters to describe the relation between the satellite and the additional signal: $\Theta = \varphi_{\mathrm{add}} - \varphi_{\mathrm{sat}}$ describes the carrier-phase offset and $\alpha = \frac{A_{\mathrm{add}}}{A_{\mathrm{sat}}}$ describes the amplitude ratio of the additional signal compared to the satellite signal. In general, it is more common to describe the relationship between two signals by the relation of their power. The power is proportional to the square of the amplitude. Hence, further on, we will use the square of the amplitude ratio α^2 instead of the amplitude ratio α to describe the relation between the satellite and the additional signal.

The factor before the square brackets in Equation (3) is independent of the lag value τ and works as a scaling factor. It can be neglected because it has no influence on the zero crossing of the S-curve (the importance of the zero crossing will be described in Section 3.3). In addition, as described in Section 2, we assume for now that the relative frequency offset is zero (i.e., $f_{\mathrm{sa}} = 0\,\mathrm{Hz}$). The ambiguity function can therefore be simplified to:

$$S'_{\Sigma}(\tau) = R(\tau) + \alpha e^{-\mathrm{j}\Theta} R(\tau - d_{\mathrm{sa}}) \tag{4}$$

3.2 | S-Curve and Autocorrelation Function

Following the nomenclature of Van Nee (1993), a non-coherent early-late discriminator (S-curve) can be defined as:

$$D(\tau) = \left| S'_{\Sigma}\left(\tau + \frac{d_{\mathrm{c}}}{2}\right) \right| - \left| S'_{\Sigma}\left(\tau - \frac{d_{\mathrm{c}}}{2}\right) \right| \tag{5}$$

$$\begin{aligned} &= \left| R\left(\tau + \frac{d_{\mathrm{c}}}{2}\right) + \alpha R\left(\tau + \frac{d_{\mathrm{c}}}{2} - d_{\mathrm{sa}}\right) e^{-\mathrm{j}\Theta} \right| \\ &\quad - \left| R\left(\tau - \frac{d_{\mathrm{c}}}{2}\right) + \alpha R\left(\tau - \frac{d_{\mathrm{c}}}{2} - d_{\mathrm{sa}}\right) e^{-\mathrm{j}\Theta} \right| \end{aligned} \tag{6}$$

where d_{c} is the correlator spacing of the discriminator in units of chips defining the offset of the early and late correlators with respect to the tracked PRN code phase. Traditionally, the autocorrelation function for GPS L1 C/A—to calculate the MEE—is approximated by a triangular-shaped function centered around zero (Van Nee, 1992). This function is zero outside of the triangular shape. However, Braasch (1997) points out that the autocorrelation function for a PRN sequence with a finite length has non-zero sidelobes. He demonstrated the relevance of these sidelobes on the code tracking error for a multipath signal. We follow the suggestion of Braasch (1997) and use the following approximation for the normalized autocorrelation function of the PRN codes:

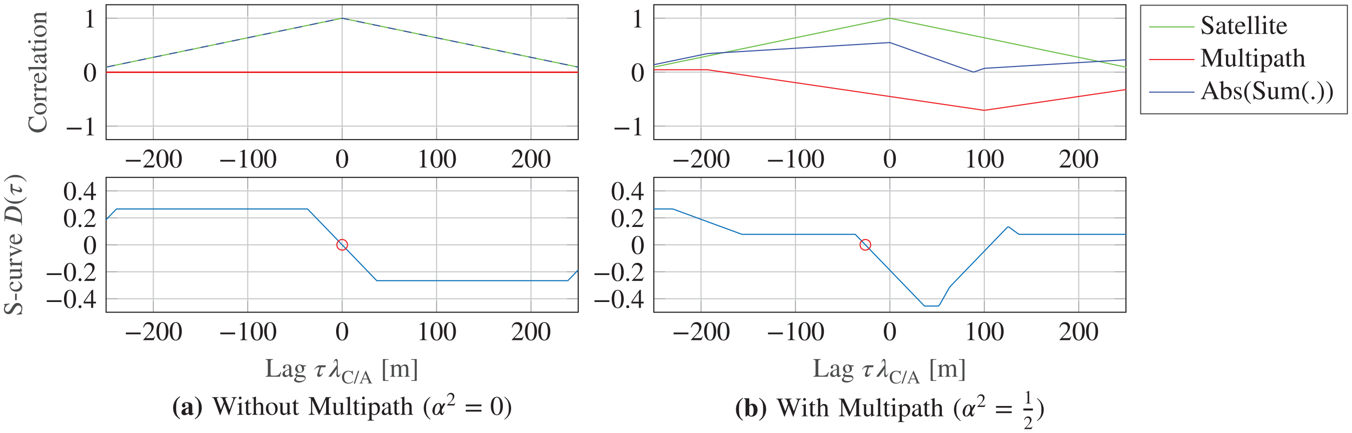
$$R(\tau)=\begin{cases}1+(\Gamma-1)|\tau| & |\tau|\leq 1\\ \Gamma & \text{otherwise}\end{cases} \tag{7}$$

where τ is in units of chips and Γ represents the level of the first sidelobe of the autocorrelation function depending on the used spreading code. We postulate that the sidelobe level is smaller than the main peak (i.e., $|\Gamma|<1$). In the case of GPS L1 C/A, three sidelobe levels are possible. The normalized sidelobe levels are $-\frac{1}{1023}$, $-\frac{65}{1023}$, and $\frac{63}{1023}$.

It shall be emphasized that the defined quantities τ, d_c, and d_{sa} are in units of chips. However, to get a better feeling for the corresponding values in a positioning context, the lag value τ and the relative delay d_{sa} will be stated in meters, i.e., multiplied with the chip length of the GPS L1 C/A code: $\lambda_{C/A}=293.26\frac{\text{m}}{\text{chip}}$.

3.3 | Stable and Unstable Tracking Points

To understand the effect of distortion on the S-curve, it is helpful to look at two examples. The top plots in Figure 1 show the (approximated) autocorrelation function for the satellite (green line), the additional signal (red line), and the absolute value of the sum of these two functions (blue line). The bottom plots show the corresponding S-curves: The output of the non-coherent early-late discriminator as shown in Equation (6). In the undistorted case (Figure 1a), the power of the additional signal is zero (i.e., $\alpha^2=0$).



(a) Without Multipath ($\alpha^2=0$)

(b) With Multipath ($\alpha^2=\frac{1}{2}$)

FIGURE 1 Correlation triangles (top) and S-curve (bottom) for a satellite signal and its multipath with $\alpha^2=0$ (a) and $\alpha^2=\frac{1}{2}$ (b), respectively; the relative signal delay of the multipath is $d_{sa}\lambda_{C/A}=100$ m and the correlator spacing $d_c=0.25$ ($d_c\lambda_{C/A}\approx 73.24$ m). The red circle marks the relevant stable tracking point of the scenario.

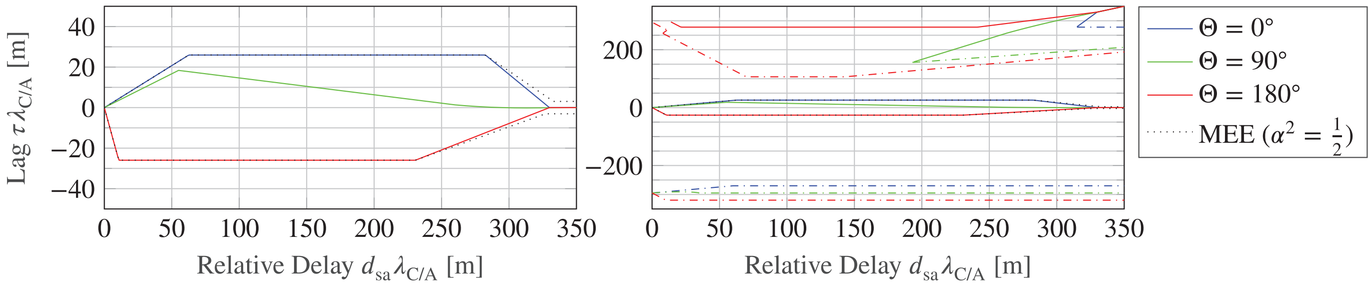
The discriminator output can be used to steer the local replica: If it is positive $(D(\tau) > 0)$, the replica will be delayed, and if it is negative $(D(\tau) < 0)$, the replica will be advanced. Due to this mechanism, the DLL will track a position in the S-curve where $D(\tau) = 0$ and $\frac{\mathrm{d}D(\tau)}{\mathrm{d}\tau} < 0$. We call a lag value τ fulfilling these equations' stable tracking points. In the bottom plot, it is marked by a red circle. In the undistorted example, this is fulfilled at a delay of $\tau\,\lambda_{\mathrm{C/A}} = 0$ m, enabling the DLL to keep the replica matched with the incoming signal.

In the distorted case (Figure 1[b]), the additional signal has half the power of the satellite signal $(\alpha^2 = \frac{1}{2})$. It is delayed by $d_{\mathrm{sa}}\lambda_{\mathrm{C/A}} = 100$ m and its carrier is in counter phase to the satellite signal (i.e., $\Theta = 180°$). In this example, the discriminator output is negative when the local replica matches the satellite signal. The mechanism assumes that the replica is delayed and advances it until the discriminator becomes zero or positive. That is fulfilled for a delay of about $\tau\,\lambda_{\mathrm{C/A}} = -26$ m. In the bottom plot, this stable tracking point is again marked with a red circle. Due to the distorion of the S-curve, in this example, the multipath causes a code tracking error of about $\tau\,\lambda_{\mathrm{C/A}} = 26$ m.

Complementary to the stable tracking points, we call a position in the S-curve, where $D(\tau) = 0$ and $\frac{\mathrm{d}D(\tau)}{\mathrm{d}\tau} > 0$, an unstable tracking point. Theoretically, a DLL could settle on such a point, because the discriminator function is zero. However, even the smallest offset to this point drives the DLL away from this position due to the sign of the discriminator function.

3.4 | Recap of Multipath Error Envelope

The idea of the Multipath Error Envelope (MEE) is to calculate the stable tracking points as a function of the amplitude ratio α, the relative signal delay d_{sa}, and the correlator spacing d_{c} (Van Nee, 1992). To get rid of the relative phase offset, the MEE is defined using the worst-case tracking bias over the phase offsets. Again, it is helpful to look at an example: Figure 2(a) shows the course of the stable tracking points over the relative delay for the in-phase ($\Theta = 0°$, solid blue line), the counter-phase ($\Theta = 180°$, solid red line), and one phase in-between ($\Theta = 90°$, solid green line). The plot is the result of solving the S-curve for zero crossings $(D(\tau) = 0)$ using the definition of Equation (6) with Equation (7). A fixed amplitude ratio, correlator spacing, and sidelobe level have been used.



(a) Zoomed in **(b)** Zoomed out

FIGURE 2 Lag values resulting in zero crossings of the S-curve as a function of the relative delay of the multipath; calculated for $\Theta \in \{0°; 90°; 180°\}$, $d_{\mathrm{c}} = 0.25$, $\alpha^2 = \frac{1}{2}$, and $\Gamma = \frac{-65}{1023}$; the solid line marks a zero crossing with a negative slope (stable tracking points) and the dash-dotted line marks a zero crossing with a positive slope (unstable tracking points). Figure (a) limits the y-axis to a range from −50 m to 50 m, whereas Figure (b) shows a range from −350 m to 350 m.

The two curves corresponding to the in-phase (blue) and the counter-phase (red) cases form the well-known MEE. Van Nee (1992) identified these cases to be the worst regarding the tracking bias and used them to define the upper and lower bounds. Next to the calculated courses of the zero crossings, Figure 2(a) shows the MEE as suggested by Braasch (1997) as a black dotted line. The first two line segments of the envelope matches with the course of the zero crossings for in-phase (blue line) and counter-phase (red line). This is similar to the MEE of Van Nee (1992). For the last two line segments, Braasch considered the worst-case change of the sidelobes in the autocorrelation function to overbound the tracking error for large relative delays of the multipath echo. In contrast, the calculated course of the zero crossings (blue and red line) is used in Equation (7) to approximate the autocorrelation function. This approximation is limited to constant instead of changing sidelobes.

Figure 2(b) shows the same plots, but zooms out and reveals additional solutions for $D(\tau) = 0$. In addition to the stable tracking points (solid lines), the unstable tracking points are plotted as dash-dotted lines. If we focus, for example, on the counter-phase case, we can see that there are courses for two different stable tracking points (upper and lower solid red lines). To determine which one will be tracked, it is helpful to take a look at unstable tracking points. Due to the working mechanism of the DLL (see Section 3.3), we can formulate the following rule:

> On a vertical axis, the next stable tracking point that can be reached without crossing an unstable tracking point will be tracked.

With this rule, it becomes obvious that it matters in which state the code tracking was in before the additional signal comes into play. It is reasonable to expect that the satellite signal was tracked before the multipath occurs $(\tau = 0)$. With the defined rule and the starting position, it is straightforward to evaluate the expected tracking error in the example (Figure 2). Going back to the counter-phase case (red lines), we can now say that (starting from $\tau = 0$) the lower stable tracking point will be tracked and not the upper one.

At this point, it should be emphasized that the MEE is only valid under the assumption that the power of the additional signal is less than the power of the satellite signal $(\alpha^2 < 1)$. This assumption is reasonable for a multipath signal, because a multipath signal is a reflection and, therefore, usually less powerful than the original line-of-sight signal—unless the latter one is further attenuated, for example, by shadowing. However, this assumption does not hold for a spoofing signal.

4 | CONSIDERATIONS RELEVANT FOR DERIVING THE SPOOFER ERROR ENVELOPE

This section extends the concept of the MEE to an additional signal that is more powerful than the authentic satellite signal $(\alpha^2 > 1)$. To distinguish the additional signal from a multipath, we call it a spoofing signal, even though a spoofing signal could also have less power.

This section is divided into two subsections. The first subsection (4.1) demonstrates some challenges in deriving a Spoofer Error Envelope (SEE) compared to the MEE using an exemplary parameter set. The second subsection (4.2) extends this demonstration to six parameter sets and gives a numerically calculated bound of the tracking offset in the presence of a spoofing signal.

4.1 | Effect of a Spoofing Signal on the S-Curve

In order to estimate the SEE, it is helpful to take a look at the S-curve in the presence of a spoofing signal. Figure 3 shows the correlation triangles and the S-curves for two different scenarios.

The setup is similar to the one of Figure 1(b), but the additional signal is more powerful relative to the authentic signal ($\alpha^2 = 2$ compared to $\alpha^2 = \frac{1}{2}$). The left scenario differs from the right scenario only by one parameter: In the left plots, a relative delay of $d_{\mathrm{sa}}\lambda_{\mathrm{C/A}} = 100$ m is used and in the right plots, $d_{\mathrm{sa}}\lambda_{\mathrm{C/A}} = 120$ m. For code tracking, this little change makes a huge difference. At this point, we want to recall the assumption that the receiver tracks the authentic signal before the spoofing signal is superposed (i.e., initially $\tau = 0$).

In the left scenario, the discriminator output is positive for a lag value of zero ($D(\tau = 0) > 0$). Therefore, the code replica in the receiver will be delayed until the discriminator output becomes zero at about $\tau\lambda_{\mathrm{C/A}} = 126$ m (red circle in the left plot). Whereas in the right scenario, the discriminator output is negative for a lag value of zero ($D(\tau = 0) < 0$), resulting in a reduction of the delay until it reaches about $\tau\lambda_{\mathrm{C/A}} = -158$ m (red circle in the right plot). Summing up, in this example, a difference of 20 m in the relative delay between the satellite and the spoofing signal results in a tracking difference of about 284 m.

In the next step, we consider not only two, but a range of relative delays. Figure 4 plots the lag values yielding zeroes of the discriminator function (stable and unstable tracking points) over the relative signal delay.

At this point, we want to recall the earlier established rule governing how to read these plots from Section 3.4. From an arbitrary point in the plot, the next stable tracking point in the vertical direction (without crossing an unstable one) will be tracked. Applying this rule, one can determine the expected code tracking bias as a function of the relative delay. (To check the result: The expected tracking bias for this scenario is plotted in the left-center plot of Figure 5). In contrast to the expected bias in a multipath scenario, this function is not continuous. In the counter-phase case (red), a jump occurs at about $d_{\mathrm{sa}}\lambda_{\mathrm{C/A}} = 112$ m. Before this point ($d_{\mathrm{sa}}\lambda_{\mathrm{C/A}} < 112$ m), the upper solid red line will be tracked and after this point the lower solid red line will be tracked. For the in-phase case (blue), a similar jump occurs at about $d_{\mathrm{sa}}\lambda_{\mathrm{C/A}} = 317$ m.

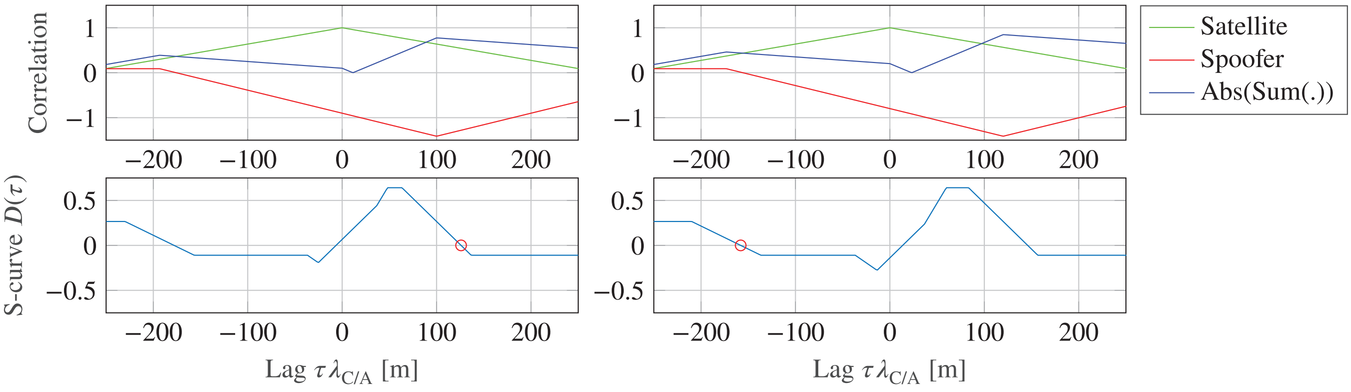


FIGURE 3 Correlation triangles (top) and S-curve (bottom) for a satellite and a spoofing signal with $\alpha^2 = 2$ and a signal delay of $d_{\mathrm{sa}}\lambda_{\mathrm{C/A}} = 100$ m (left) and $d_{\mathrm{sa}}\lambda_{\mathrm{C/A}} = 120$ m (right), respectively; a correlator spacing of $d_{\mathrm{c}} = 0.25$ ($d_{\mathrm{c}}\lambda_{\mathrm{C/A}} \approx 73.24$ m) is used. The red circle marks the relevant stable tracking point of the scenario.

Please note that such a jump does not mean that a receiver that tracks the upper tracking point will be driven to the lower one as the relative delay of the spoofing signal grows. Once locked onto a tracking point, the receiver will continue to stay on it and follow, for example, the upper curve. However, the receiver will lock onto the tracking point on the lower curve if the spoofer appears with a relative delay behind the position of the jump. Hence, the relative delay of the spoofing signal determines which curve (upper or lower) the receiver will follow.

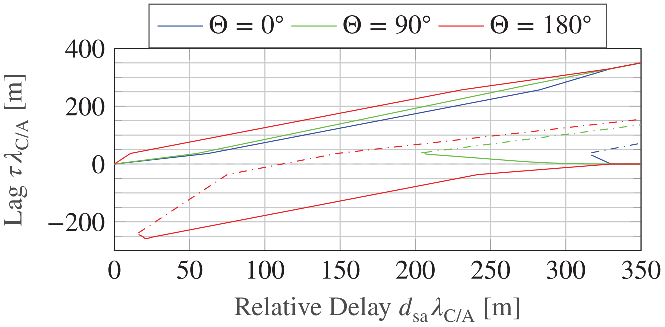


FIGURE 4 Lag values resulting in zero crossings of the S-curve as a function of the relative delay of the spoofing signal; calculated for $\Theta \in \{0°; 90°; 180°\}$, $d_c = 0.25$, $\alpha^2 = 2$ and $\Gamma = \frac{-1}{1023}$. The solid line marks a zero crossing with a negative slope (stable tracking points) and the dash-dotted line marks a zero crossing with a positive slope (unstable tracking points).

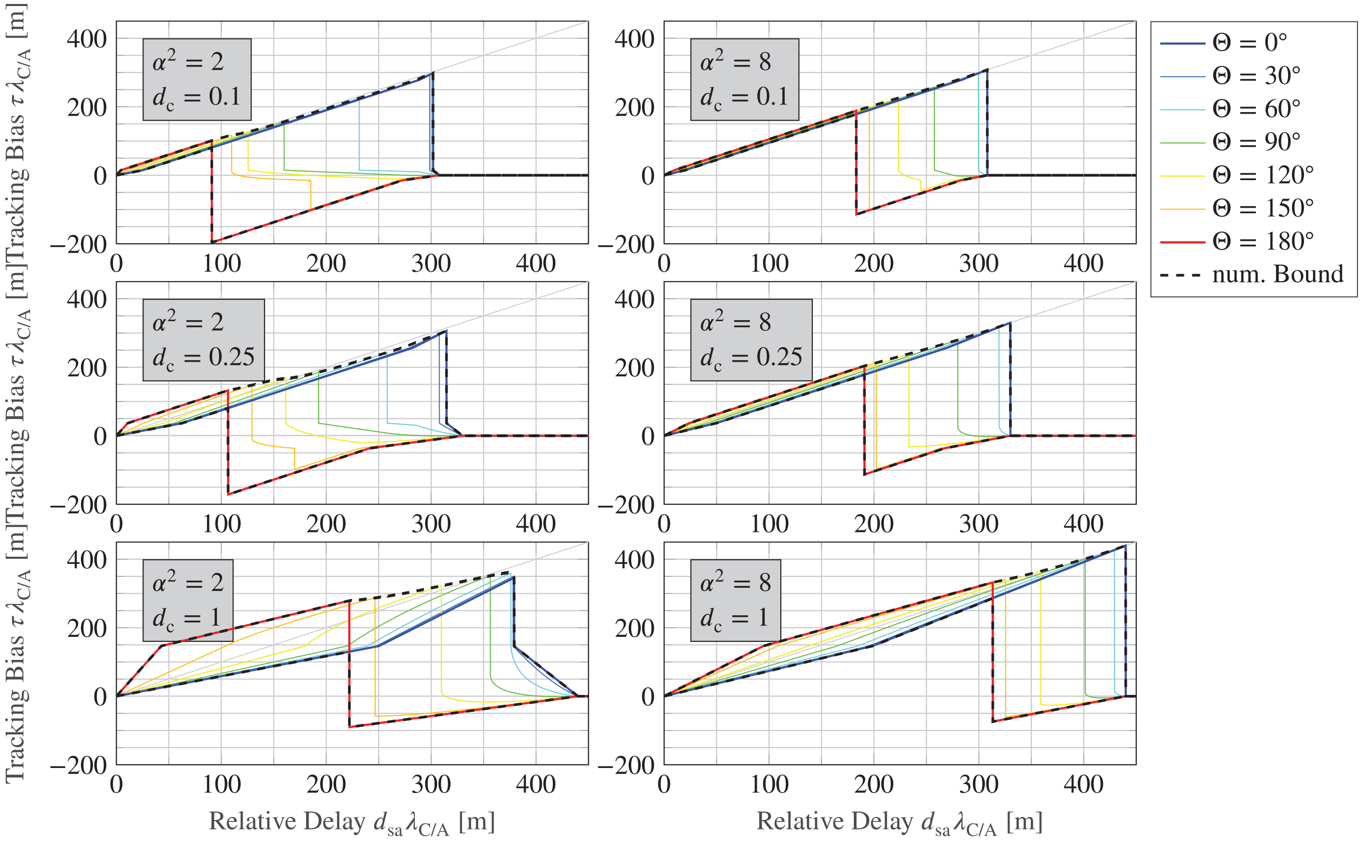


FIGURE 5 Expected code tracking bias based on the stable tracking points for different power ratios and correlator spacings; the left plots are simulated using a power ratio of $\alpha^2 = 2$ and the right plots $\alpha^2 = 8$. Vertically, the used correlator spacing varies from $d_c = 0.1$ (top) over $d_c = 0.25$ (center) to $d_c = 1$ (bottom). Each plot shows the bias for a number of carrier-phase offsets ($\Theta \in \{0°; 30°; 60°; 90°; 120°; 150°; 180°\}$) and a numerical calculated bound.

4.2 | Numerical Bounds for Tracking Error

Although Figure 4 allows for a first step towards a Spoofer Error Envelope, it still represents only a single set of parameters. To get a broader picture, Figure 5 shows the results for six scenarios with a larger variety of carrier-phase offsets ($\Theta \in \{0°; 30°; 60°; 90°; 120°; 150°; 180°\}$). In these scenarios, the relative power of the spoofing signal ranges from $\alpha^2 = 2$ to $\alpha^2 = 8$ and the correlator spacing ranges from $d_c = 0.1$ to $d_c = 1$.

Plotting all stable and unstable tracking points would be confusing due to the number of graphs. Instead, the plots show only the stable tracking points that will be tracked according to the rule defined in Section 3.4. Therefore, we no longer call the lag value *lag* but rather the *expected code tracking bias* or, for short, *tracking bias*. To get the tracking bias, two steps are conducted:

1. The sign of $D(\tau = 0)$ is checked to determine if the lag value of the relevant stable tracking point is above ($\tau > 0$) or below ($\tau < 0$) zero.
2. The location of the next stable tracking point in the determined direction is numerically calculated using the properties $D(\tau) = 0$ and $\frac{\mathrm{d}D(\tau)}{\mathrm{d}\tau} < 0$.

Figure 5 shows a numerically calculated bound for the code tracking bias as a black dashed line. This bound gives the minimal and maximal tracking bias over the carrier-phase offsets. For the shown bound, the carrier-phase offsets from −180° to 180° with a step size of 1° were considered.

The question we want to examine is: Can a worst-case tracking bias be described using only the in-phase and the counter-phase cases of the relative carrier phase? Therefore, we compare the numerical bound with the curves of these two cases.

Looking at the six scenarios in Figure 5, the lower numerical bound (lower black dashed line) can exclusively be described by the in-phase (blue line) and the counter-phase (red line) cases: The first two (bottom-left plot) line segments of this bound are given by the in-phase case. The remaining segments (after the jump) are given by the counter-phase case.

The upper numerical bound (upper black dashed line), on the other hand, is more tricky: Though the first two line segments of this bound can be described by the counter-phase case (red line), the next segment depends on different relative carrier phases. The following line segments (after the jump of the upper bound) can be described by the in-phase case (blue line). At this point, it is noteworthy that, even though it is not plotted, the upper stable tracking point of the counter-phase case (red line before the jump) is still present after the jump. Its ongoing course can be seen, for example, in Figure 4 (upper solid red line). In Figure 5, the corresponding curve stops at the jump because, at larger relative delays d_{sa}, the DLL switches to another stable tracking point as discussed in Section 4.1.

However, due to its course, it is useful for defining a non-tight upper bound even after the jump. Summing up, according to the six scenarios, a non-tight bound can be expressed exclusively by the in-phase and the counter-phase cases.

5 | SPOOFER ERROR ENVELOPE

Based on the results of the previous sections, in this section we will define the Spoofer Error Envelope (SEE) for the non-coherent early-late discriminator

(Section 5.1). The SEE is an analytical bound of the expected tracking bias induced by a spoofer. The second part of this section compares the defined bound with a numerical bound (Section 5.2) and simulation results from a receiver implementation (Section 5.3).

In addition to the results from the previous section, the concept of Braasch (1997) will be reused to define the bound for large delays d_{sa}. For delays larger than $1+\frac{d_{\mathrm{c}}}{2}$, he found the bound to be:

$$\pm\alpha \frac{d_{\mathrm{c}}}{2}\frac{\Gamma_{\max}-\Gamma_{\min}}{1-\Gamma} \tag{8}$$

where $\Gamma_{\max}$ and $\Gamma_{\min}$ are the maximal and minimal possible sidelobe levels of the used PRN code (the possible sidelobe levels for GPS L1 C/A are given in Section 3.2). This bound was defined for the MEE ($\alpha<1$), but also holds under the assumption that $\alpha \le \frac{1-\Gamma}{\Gamma_{\max}-\Gamma_{\min}}$. For GPS L1 C/A, the lowest limit of the ratio (given by the largest sidelobe level: $\Gamma=\frac{63}{1023}$) is $\alpha \le 7.5$ (i.e., the power of the spoofing signal compared to the satellite signal must not exceed 17.5 dB). This limit does not pose a problem because larger power ratios tend to knock out the receiver, forcing it to go into acquisition mode. However, we assumed that the receiver stays in the tracking state (compare to Section 2.3).

5.1 | Defining a Spoofer Error Envelope

The expected tracking bias can be determined by finding stable tracking points. Stable tracking points are given solving $D(\tau)=0$, Equation (6) with (7). Including the information of the previous sections, we can identify the stable tracking points that will be tracked by the receiver depending on the initial tracking conditions and parameters. For this SEE, we assume that the authentic signal is tracked prior to the addition of the spoofing signal and that the correlator spacing is between zero and one chip ($0<d_{\mathrm{c}}\le 1$).

Complementary to the MEE, we postulate that the spoofer-to-authentic signal power is greater than one ($\alpha^2>1$) and, in order to reuse the bound of Braasch (1997) for long delays: $\alpha \le \frac{1-\Gamma}{\Gamma_{\max}-\Gamma_{\min}}$. To give an overbound for all phase offsets, we use the bounds of the in-phase ($\Theta=0°$) and counter-phase ($\Theta=180°$) cases. This is justified by the observations in Section 4.2 and the detailed derivation in Appendix (A). Finally, a SEE can be defined as:

$$\tau_{\mathrm{SEEMax}} = \begin{cases} \dfrac{\alpha}{\alpha-1}d_{\mathrm{sa}} & 0<d_{\mathrm{sa}}\le\left(1-\frac{1}{\alpha}\right)\frac{d_{\mathrm{c}}}{2} \quad \text{(9a)} \\[2ex] d_{\mathrm{sa}}+\dfrac{d_{\mathrm{c}}}{2\alpha} & \left(1-\frac{1}{\alpha}\right)\frac{d_{\mathrm{c}}}{2}<d_{\mathrm{sa}}\le 1-\left(1+\frac{1}{\alpha}\right)\frac{d_{\mathrm{c}}}{2} \quad \text{(9b)} \\[2ex] d_{\mathrm{sa}}-\dfrac{\left(d_{\mathrm{sa}}-\frac{d_{\mathrm{c}}}{2}-1\right)\left(1-\Gamma-\Gamma_{\max}+\Gamma_{\min}\right)-d_{\mathrm{c}}\left(\Gamma_{\max}-\Gamma_{\min}\right)}{\left(1-\Gamma-\Gamma_{\max}+\Gamma_{\min}\right)+2\alpha(1-\Gamma)} & 1-\left(1+\frac{1}{\alpha}\right)\frac{d_{\mathrm{c}}}{2}<d_{\mathrm{sa}} \le 1+\frac{d_{\mathrm{c}}}{2}\left[1-\frac{\Gamma_{\max}-\Gamma_{\min}}{\alpha(1-\Gamma)}\right] \quad \text{(9c)} \\[2ex] \alpha\dfrac{d_{\mathrm{c}}}{2}\dfrac{\Gamma_{\max}-\Gamma_{\min}}{1-\Gamma} & d_{\mathrm{sa}}>1+\frac{d_{\mathrm{c}}}{2}\left[1-\frac{\Gamma_{\max}-\Gamma_{\min}}{\alpha(1-\Gamma)}\right] \quad \text{(9d)} \end{cases}$$

and

$$\tau_{\text{SEEMin}} = \begin{cases} \dfrac{\alpha}{\alpha+1} d_{\text{sa}} & 0 < d_{\text{sa}} \le \left(1+\frac{1}{\alpha}\right)\frac{d_{\text{c}}}{2} \text{ and } d_{\text{sa}} \le \frac{1}{1-\Gamma} - \frac{1}{\alpha}\left(\frac{1}{1-\Gamma} - \frac{d_{\text{c}}}{2}\right) & \text{(10a)} \\ d_{\text{sa}} - \dfrac{d_{\text{c}}}{2\alpha} & \left(1+\frac{1}{\alpha}\right)\frac{d_{\text{c}}}{2} < d_{\text{sa}} \le \frac{1}{1-\Gamma} - \frac{1}{\alpha}\left(\frac{1}{1-\Gamma} - \frac{d_{\text{c}}}{2}\right) & \text{(10b)} \\ d_{\text{sa}} - 1 + \dfrac{d_{\text{c}}}{\alpha} - \dfrac{d_{\text{c}}}{2} & \frac{1}{1-\Gamma} - \frac{1}{\alpha}\left(\frac{1}{1-\Gamma} - \frac{d_{\text{c}}}{2}\right) < d_{\text{sa}} \le 1 - \frac{d_{\text{c}}}{\alpha} & \text{(10c)} \\ \dfrac{(1-\Gamma)-\alpha\left(\Gamma_{\max}-\Gamma_{\min}\right)}{(1-\Gamma)\left(1+\frac{2}{\alpha}\right)-\alpha\left(\Gamma_{\max}-\Gamma_{\min}\right)}\left(d_{\text{sa}} - 1 + \dfrac{d_{\text{c}}}{\alpha}\right) - \dfrac{d_{\text{c}}}{2} & 1 - \frac{d_{\text{c}}}{\alpha} < d_{\text{sa}} \le 1 + \frac{d_{\text{c}}}{2}\left[1 - \frac{\alpha\left(\Gamma_{\max}-\Gamma_{\min}\right)}{1-\Gamma}\right] & \text{(10d)} \\ -\alpha \dfrac{d_{\text{c}}}{2} \dfrac{\Gamma_{\max}-\Gamma_{\min}}{1-\Gamma} & d_{\text{sa}} > 1 + \frac{d_{\text{c}}}{2}\left[1 - \frac{\alpha\left(\Gamma_{\max}-\Gamma_{\min}\right)}{1-\Gamma}\right] & \text{(10e)} \end{cases}$$

Cases (9a) and (9b) as well as (10a) and (10b) are basically the MEE from the point of view of the spoofing signal (see more details in Appendix A). Case (10c) is determined by the lower (stable) tracking point of the counter-phase. The cases (9d) and (10e) are the above mentioned bounds of Braasch (1997). Case (9c) and Case (10d) can be seen as a linear transition from Case (9b) to Case (9d) and from Case (10c) to Case (10e), respectively.

It should be noted that the formulas for the SEE are derived assuming a positive delay ($d_{\text{sa}} > 0$). However, a spoofer could also steer the signals to produce a negative delay. Due to the symmetry of the autocorrelation function, the discriminator function is odd symmetric, i.e. $D(\tau, d_{\text{sa}}) = -D(-\tau, -d_{\text{sa}})$. Hence, the function of the SEE can be continued in the negative domain of d_{sa} as an odd function, i.e., $\tau_{\text{SEEMax}}(-d_{\text{sa}}) = -\tau_{\text{SEEMax}}(d_{\text{sa}})$ and $\tau_{\text{SEEMin}}(-d_{\text{sa}}) = -\tau_{\text{SEEMin}}(d_{\text{sa}})$.

5.2 | Comparing the SEE with a Numerical Bound

The Spoofer Error Envelope is visualized in Figure 6. Additionally, a numerical bound calculated as described in Section 4.2 is shown. Comparing the numerical bound with the proposed bound in Equations (9) and (10) reveals differences:

1. A part of the upper bound of the SEE (Equation [9b] and [9c]) is larger than the numerical bound (i.e., it is a non-tight bound). The upper bound of the SEE is determined by the upper stable tracking point of the counter-phase case. After the jump of the lower bound, this tracking point is (usually) no longer reached (even though it is still a valid stable tracking point). However, the location of the jump depends on the relative phase of the spoofing signal. This results in an upper bound depending on the relative carrier phase. For the sake of simplicity, we stick to the bound defined by the counter-phase case.
2. The jump of the upper bound of the SEE (transition from [9c] to [9d]) occurs at a higher delay than in the numerical bound. It is challenging to estimate the exact location of the jump and, in practice, this jump is not sharp. Therefore, it is reasonable to choose this simplification.

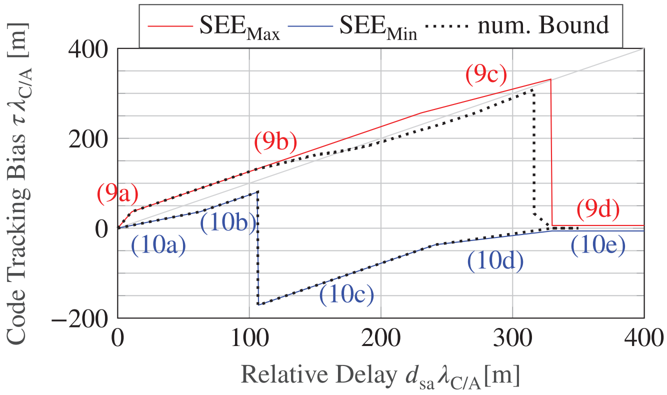


FIGURE 6 Spoofer Error Envelope with $d_c = 0.25$, $\alpha^2 = 2$; to represent a worst-case error envelope for GPS L1 C/A, the following sidelobe levels were chosen to calculate the SEE: $\Gamma = \frac{-65}{1023}$, $\Gamma_{\max} = \frac{63}{1023}$, and $\Gamma_{\min} = \frac{-65}{1023}$.

3. The jump of the lower bound (transition from [10b] to [10c]) is only tight for some parameters. As explained in Appendix A, the location of the jump is described by two different terms depending on the chosen parameters. The term chosen for the SEE describes the worst case for all parameters within the postulated ranges.

5.3 | Comparing the SEE with Simulated Tracking Errors

Besides the enumerated differences, Figure 6 gives the impression that Equations (9d), (10d), and (10e) are not tight. This results from the approximation of the autocorrelation function according to Equation (7), which has been used to calculate the numerical bound. Compared to the changing sidelobes of an exact autocorrelation function, the approximation emulates constant sidelobes. Using the autocorrelation function of some specific PRN codes (e.g., PRN 8 of GPS L1 C/A) reaches this bound as shown in Figure 7 (right plot).

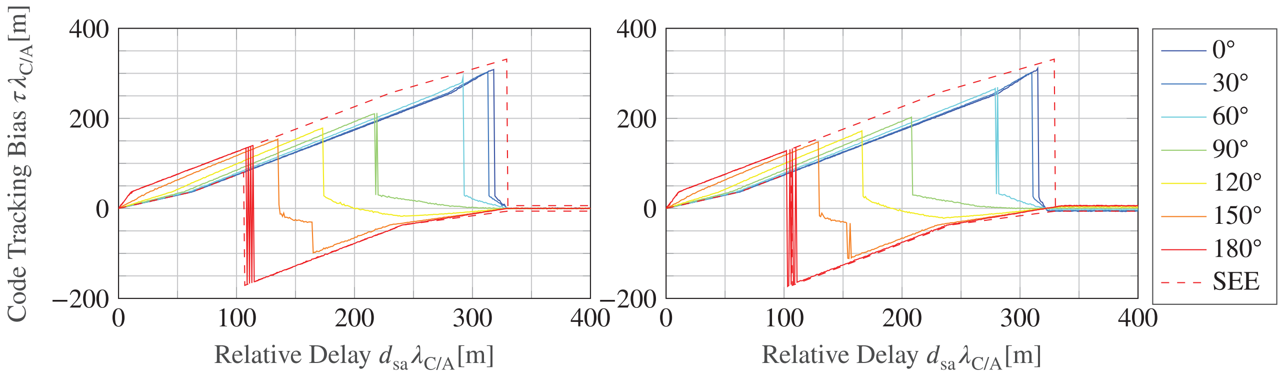


FIGURE 7 Spoofer Error Envelope and simulation results with $d_c = 0.25$, $\alpha^2 = 2$, and $\Theta \in \{0°; 30°; 60°; 90°; 120°; 150°; 180°\}$; PRN code 1 (left) and PRN code 8 (right) were used in the simulations. The simulations were conducted using the simulation tool from Bamberg et al. (2018). To represent a worst-case error envelope for GPS L1 C/A, the following sidelobe levels were chosen to calculate the SEE: $\Gamma = \frac{-65}{1023}$, $\Gamma_{\max} = \frac{63}{1023}$, and $\Gamma_{\min} = \frac{-65}{1023}$.

Figure 7 shows the SEE for a correlator spacing of $d_c = 0.25$ and with a spoofing-to-authentic signal power ratio of $\alpha^2 = 2$. Additionally, a number of simulated tracking error curves are shown for different relative carrier-phase offsets Θ between the authentic and the spoofing signal. For the simulations, the relative delay $d_{sa}\lambda_{C/A}$ was varied from 0 m to 400 m with a step size of 1 m. The resulting tracking biases are connected with line segments. The left-hand plot shows the simulation results using PRN code 1 and the right-hand plot using PRN code 8.

The simulation results demonstrate that the jumps of the bounds are not sharp. In Figure 7, this is clearly visible for the red curve $(\Theta = 180°)$. The reasons for that is simple: Signal noise. A jump results from an unstable tracking point at $\tau = 0$ as described in Section 4.1. By definition, the discriminator function is zero at the position of an unstable tracking point. Signal noise affects the discriminator output in a way that it deviates from the ideal value. At an unstable tracking point, on the other hand, a slight deviation of the discriminator output drives the DLL in a way that it drifts away from that point. The sign of the deviated discriminator value determines which stable tracking point is tracked.

Hence, the position of a jump should be interpreted as the point where the probability of tracking one or another stable tracking point is even. Due to this issue, the defined lower bound can be crossed around the jump in a simulation including signal noise.

Comparing the left-hand and the right-hand plot, it can be seen that the relative delay leading to the jump of the lower bound of the SEE depends on the used PRN code. To be more precise, it depends on the sidelobes of the autocorrelation function of the used spreading code. Regarding the position of the jump, the proposed worst-case bound is, for example, tight for PRN 8 but non-tight for PRN 1.

6 | EFFECT OF A RELATIVE DOPPLER ON THE SPOOFER ERROR ENVELOPE

To derive the Spoofer Error Envelope, which is defined in Section 5, it was postulated that the relative Doppler between the authentic and the spoofing signal is zero. In this section, the effect of a relative Doppler on the Spoofer Error Envelope will be discussed. In order to analyze this effect, it is mandatory to understand how the SEE and the MEE depend on the power ratio. Therefore, the next two subsections evaluate how these envelopes change for different power ratios. The last subsection discusses the effect of a relative Doppler on the Spoofer Error Envelope.

6.1 | The Multipath and the Spoofer Error Envelope Under Different Power Ratios

The MEE and the SEE are complementary regarding the additional-signal-to-authentic-signal power ratio. The MEE is defined for a signal weaker than the authentic signal $(\alpha^2 < 1)$ and the SEE is defined for a stronger signal $(\alpha^2 > 1)$. Figure 8 shows the MEE (left plot) and SEE (right plot) for different power ratios ranging from $\alpha^2 = \frac{1}{16}$ to $\alpha^2 = 16$. The result for the MEE is not surprisingly: A smaller power ratio results in a smaller envelope (i.e., the upper bound gets smaller and the lower bound gets larger). Due to the limited domain of the MEE $(\alpha^2 < 1)$, a maximal (inflated) MEE—the largest distance

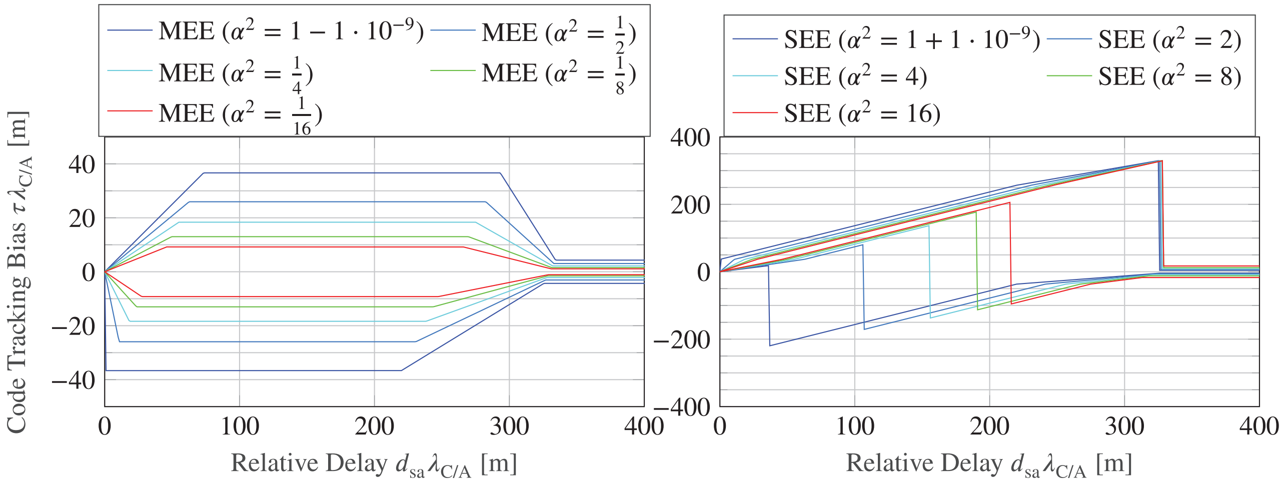


FIGURE 8 Multipath Error Envelope (left) and Spoofer Error Envelope (right) with $d_c = 0.25$ and $\alpha^2 = \left\{\frac{1}{16}; \frac{1}{8}; \frac{1}{4}; \frac{1}{2}; 0; 2; 4; 8; 16\right\}$; to represent a worst-case error envelope for GPS L1 C/A, the following sidelobe levels were chosen to calculate MEE/SEE: $\Gamma = \frac{-65}{1023}$, $\Gamma_{\max} = \frac{63}{1023}$, and $\Gamma_{\min} = \frac{-65}{1023}$.

between the upper and lower bounds—is given for a power ratio close to zero decibel $\alpha^2 \approx 1$.

The result for the SEE is more complex. Two contrary behaviors can be distinguished:

1. For large relative delays, the change of the SEE is similar to the change for the MEE: A smaller power ratio results in a smaller envelope. *Large relative delay* here means a part of the bound after the jump occurred. In Figure 8, this applies to relative delays larger than about 330 m for the upper bound. For the lower bound, the jump highly depends on the power ratio: A larger power ratio results in a jump farther to the right.
2. The upper bound of the SEE for small relative delays (in this example, smaller than about 330 m) becomes smaller and the lower bound before the jump becomes larger for larger power ratios: The envelope shrinks. At first glance, this seems to be counter-intuitive. However, these parts of the bound are basically an MEE from the point of view of the spoofing signal and, from this point of view, a larger power ratio of the spoofing signal means that the multipath signal (actually the satellite signal) becomes relatively weaker. In other words, for a large power ratio, the SEE is smaller, because the spoofing signal is more dominant and can be tracked more precisely. In contrast to 1, a small power ratio results in more uncertainty and due to the limited domain the maximal (inflated) SEE, in this case, is given for a power ratio close to zero decibels.

Summing up, the MEE and parts of the SEE reach a worst-case bound regarding the tracking bias for the case that the satellite and the additional signal power are approximately equal. However, both envelopes are not defined for a power ratio of zero decibels and, looking at Figure 8, the envelopes do not merge for power ratio close to zero decibels. The transition from the MEE to the SEE is the topic of the next section.

6.2 | Transition From Multipath to Spoofer Error Envelope

To understand why the MEE does not merge to the SEE for equally powered signals, it is helpful to plot the correlation triangle and the S-curve for such a case. Figure 9 shows these plots for the counter-phase case $(\Theta = 180°)$ and a relative signal delay of $d_{\mathrm{sa}}\lambda_{\mathrm{C/A}} = 100$ m.

At this point, it is helpful to recall the mechanism of how the DLL works (compare with Section 3.3). Due to the negative discriminator output for a zero lag $(D(0) < 0)$, the DLL will advance the replica signal. The next stable tracking point is reached at about −37 m. However, it can be observed that there is not only a single stable tracking point in the S-curve, but a large plateau with $D(\tau) = 0$ (red ellipse). On this plateau, the DLL is mainly driven by noise so that it is not possible to determine where on the plateau the DLL will stop. Therefore, the resulting tracking bias for this case can only be given as a range. In the example (Figure 9), the range is $-160\ \mathrm{m} \leq \tau\,\lambda_{\mathrm{C/A}} \leq -37$ m. A lower power ratio $(\alpha < 1)$ results in a single stable tracking point at about −37 m and a higher power ratio $(\alpha > 1)$ in a single stable tracking point at about −160 m.

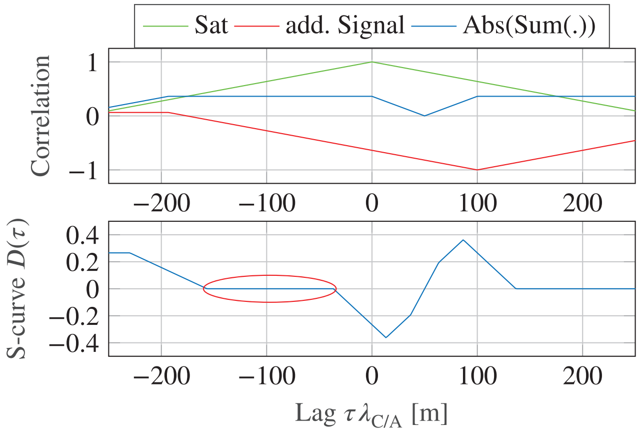


FIGURE 9 Correlation triangles (top) and S-curve (bottom) for a satellite and a spoofing signal with $\alpha^2 = 1$ and a signal delay of $d_{\mathrm{sa}}\lambda_{\mathrm{C/A}} = 100$ m; the counter-phase case is presented $(\Theta = 180°)$

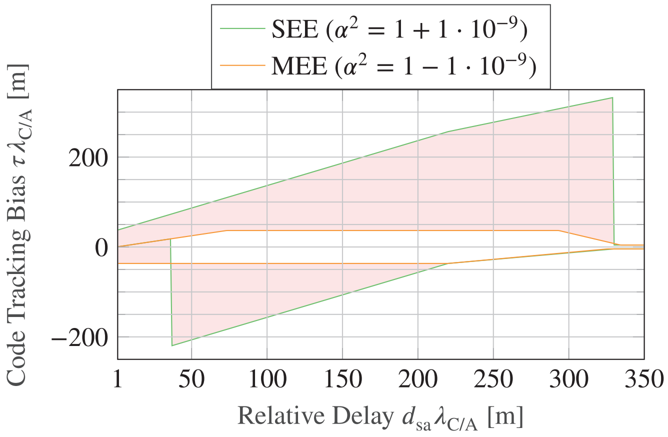


FIGURE 10 Spoofer Error Envelope and Multipath Error Envelope with $d_c = 0.25$ and $\alpha^2 \approx 1$; to represent a worst-case error envelope for GPS L1 C/A, the following sidelobe levels were chosen to calculate MEE/SEE: $\Gamma = \frac{-65}{1023}$, $\Gamma_{\max} = \frac{63}{1023}$, and $\Gamma_{\min} = \frac{-65}{1023}$.

Figure 10 plots the MEE and the SEE for an additional-signal-to-authentic-signal power ratio of one ($\alpha = 1$).

The discrepancy between both envelopes is filled red. Even though some of the discrepancy results from the non-tight bounds of the defined SEE (see Section 5.1), it is mainly caused by the aforementioned plateaus of zero values. In practice, the transition at ($\alpha = 1$) is not sharp. The closer the power ratio is to unity, the higher the probability that an arbitrary point of the plateau is tracked. So the transition can only be described by a random process for power ratios close to unity.

6.3 | The Effect of a Relative Doppler

In Section 4, it was described how a GNSS receiver correlates the incoming signal with a local replica of the code and carrier signal to track the signal. The result of this correlation is mathematically described by the Ambiguity Function. In Section 4, it was assumed that the relative carrier frequency offset between the satellite and the spoofing signal was zero ($f_{\mathrm{sa}} = 0\,\mathrm{Hz}$). Therefore, the simplified ambiguity function read (recall of Equation [4]):

$$S'_{\Sigma}(\tau) = R(\tau) + \alpha e^{-\mathrm{j}\Theta} R(\tau - d_{\mathrm{sa}}) \tag{11}$$

In this section, the relative carrier frequency offset plays a role. Hence, Equation (3) can only be simplified to:

$$S''_{\Sigma}(\tau) = R(\tau) + \alpha \frac{\mathrm{sinc}((f_{\mathrm{o}} - f_{\mathrm{sa}})T_c)}{\mathrm{sinc}(f_{\mathrm{o}} T_c)} e^{-\mathrm{j}\Theta(t)} R(\tau - d_{\mathrm{sa}}) \tag{12}$$

Equation (11) and Equation (12) differ in two significant respects:

1. The relative phase offset (Θ) in Equation (12) is time-dependent: In Equation (11) we assumed no relative carrier frequency offset, so that the relative phase offset was constant. With a relative carrier frequency offset, the relative phase offset varies.
2. The power ratio of the spoofing signal to the satellite signal is affected by the relative Doppler offset (f_{sa}) and by the tracking mismatch of the carrier tracking loop to the satellite signal (f_{o}).

With the preliminary studies in the previous sections, we now have enough tools to discuss the effect of a relative Doppler on the Spoofer Error Envelope. For all of the following considerations, we presume that the tracking in the receiver is in a stable state and especially that the receiver has not lost lock. The expected tracking error in the presence of a spoofing signal depends on the relative Doppler:

1. For **small relative Doppler offsets**, the effect of the sinc-function in Equation (12) is negligible. It is postulated that the phase lock loop (PLL) tracks the satellite signal ($f_{\mathrm{o}} = 0\,\mathrm{Hz}$) before the spoofing signal is switched on and the sinc-function (in the denominator) is approximately unity for small values. Due to a changing phase offset Θ, the (relevant) stable tracking point of the S-curve rotates between the in-phase and the counter-phase case. The positions of the stable tracking points for varying phase offsets are visualized in Figure 5 and Figure 7 for some examples. Due to the relatively slow-changing phase offset, the DLL manages to follow the stable tracking points. Hence, the

expected tracking bias for small relative Doppler offsets is within the bounds of the SEE. With an increasing relative Doppler offset (greater than the DLL loop bandwidth), the DLL averages the code tracking error until it converges to a single bias. As Kelly et al. (2003) and Van Nee (1993) demonstrated, the resulting bias is not necessarily the midpoint of the upper and lower bound of the MEE. Due to the similarities of the envelopes, the same can be expected for the averaged SEE bias.

2. For **medium relative Doppler offsets**, the effect of the sinc-function in Equation (12) is no longer negligible. Therefore, it can occur that a spoofing signal, which is more powerful than the satellite signal, appears to be equally strong or even weaker than the satellite signal. In such a case, the MEE needs to be considered as well. Even if the spoofing signal still appears to be more powerful than the satellite signal, the bounds of the SEE would need to be adapted to a lower power ratio (because the spoofing signal is attenuated in the correlation process). On the other hand, if the spoofing signal still appears stronger, it is most likely that the PLL will adapt to the spoofing signal (at least, if it is within the pull-in range of the PLL). This turns over the effect of the sinc-function factor to the favor of the spoofing signal and the power ratio α appears to be higher than it actually is. In this case, the SEE needs to be adapted as well. Summed up, the bounds for the tracking error are an overbound of the worst-case MEE (reached at about $\alpha^2 = 1$) and/or a mixture of two SEEs (one for the highest and one for the lowest possible power ratio). If the DLL tracks the spoofing signal but the Doppler of the spoofing signal is outside of the pull-in range of the PLL, the PLL might even lose lock. Depending on the implementation in the receiver, this leads to a re-acquisition of the satellite signal.
3. For **large relative Doppler offsets**, the effect of the sinc-function in Equation (12) is significant. Due to the postulation that the receiver tracks the satellite signal $(f_o = 0\,\text{Hz})$ before the spoofing signal is switched on, the spoofing signal will appear (significantly) weaker than the satellite signal. Due to the low signal power, the PLL will continue to track the satellite signal. Therefore, instead of the spoofer, the Multipath Error Envelope needs to be considered. The power ratio for this resulting MEE can be calculated by considering the relative frequency offset, i.e., $\alpha' = \alpha\,\text{sinc}(f_{sa}T_c)$. The effect of a relative Doppler offset on a multipath signal has been analyzed by Kelly et al. (2003). The results can directly be applied to this case here.

Figure 11 shows some of the simulation results conducted with the simulation tool from Bamberg et al. (2018). It plots the experienced tracking bias over the relative code delay between the satellite signal and the spoofing signal for different relative Doppler offsets. The experienced tracking bias is averaged over one second. For each relative delay and for each Doppler offset, one simulation was conducted. Additionally, the SEE was plotted for comparison. At this point, it should be noted that the tracking errors for which the receiver detected a loss of lock of the tracked satellite are not shown in the plot. Consequently, some plots show gaps (e.g., $f_{sa} = 40\,\text{Hz}$).

The plots in Figure 11 confirm the conclusions of this section: For small relative Doppler offsets, an averaged tracking bias of the SEE bounds is observed $(f_{sa} = 10\,\text{Hz},\ 25\,\text{Hz, and}\ 40\,\text{Hz})$. For medium relative Doppler offsets, the receiver tends to lose lock; however if not, the tracking error would be between the SEE and the MEE $(f_{sa} = 55\,\text{Hz},\ 70\,\text{Hz, and}\ 85\,\text{Hz})$. For large relative Doppler offsets, an average of the bounds of the MEE is tracked (e.g.,

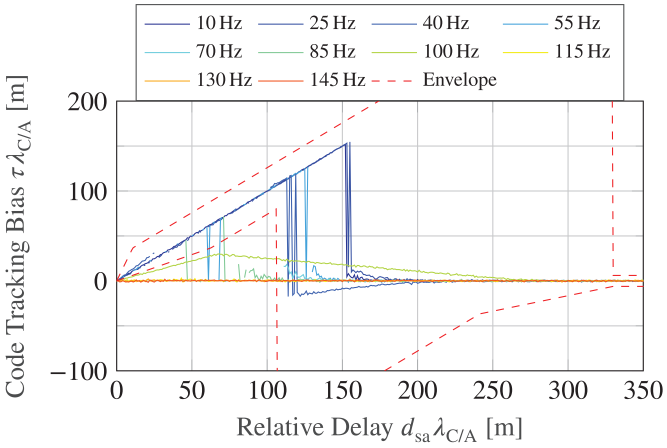


FIGURE 11 Spoofer Error Envelope and simulation results with $d_c = 0.25$, $\alpha^2 = 2$, and f_{sa} from 0 Hz to 150 Hz using PRN code 8; the simulations were conducted using the simulation tool from Bamberg et al. (2018). The implemented tracking module used a coherent integration time of $T_c = 5$ ms, a PLL bandwidth of 15 Hz, and DLL bandwidth of 1 Hz. To represent a worst-case error envelope for GPS L1 C/A, the following sidelobe levels were chosen to calculate the SEE: $\Gamma = \frac{-65}{1023}$, $\Gamma_{max} = \frac{63}{1023}$, and $\Gamma_{min} = \frac{-65}{1023}$.

$f_{sa} = 100$ Hz, 115 Hz, 130 Hz, and 145 Hz). The last mentioned plots show the same shape as the multipath errors for relative Doppler offsets (Braasch, 1992; Kelly et al., 2003; Van Nee, 1993), especially the plot for $f_{sa} = 100$ Hz. These results are in line with the findings of Kelly et al. (2003), who concluded that the average tracking bias becomes smaller for higher Doppler offsets (even in the context of a non-coherent discriminator).

7 | GENERALIZED TRACKING BOUND

The Spoofer Error Envelope (SEE) was derived under the assumption that the relative delay between the spoofing signal and the authentic signal would stay approximately constant (see Section 2.3). However, this assumption is not always fulfilled. Due to satellite movement, dynamics of the user, active steering of the spoofer, etc., the quasi-static relative delay only holds for a limited amount of time. In this sense, the SEE bounds only an initial tracking error. In this section, we derive a more generalized tracking bound that accounts for time-varying relative delays between spoofing and authentic signals.

The main concept used to derive the SEE still applies to this generalized bound: The DLL tracks a position where the discriminator function is zero and has a negative slope (i.e., a stable tracking point [see Section 3.3]). Therefore, the positions of stable tracking points stay the same as in the case of the SEE. Also, the rule introduced in Section 3.4—defining at which stable point the DLL settles—still applies. However, in the case of the generalized bound, the DLL is not necessarily assumed to track the authentic signal and, therefore, the search for the next tracking point of the DLL can start from $\tau \neq 0$. For example, due to the previous spoofing effect, the DLL may settle on some lag value τ_1 within the bounds of the SEE. If the relative delay changes, τ_1 needs to be considered as the new starting point. Hence, for a generalized bound, we need to consider all stable tracking points and not only those that are reached with a starting point at $\tau = 0$ (as done in Section 4.1).

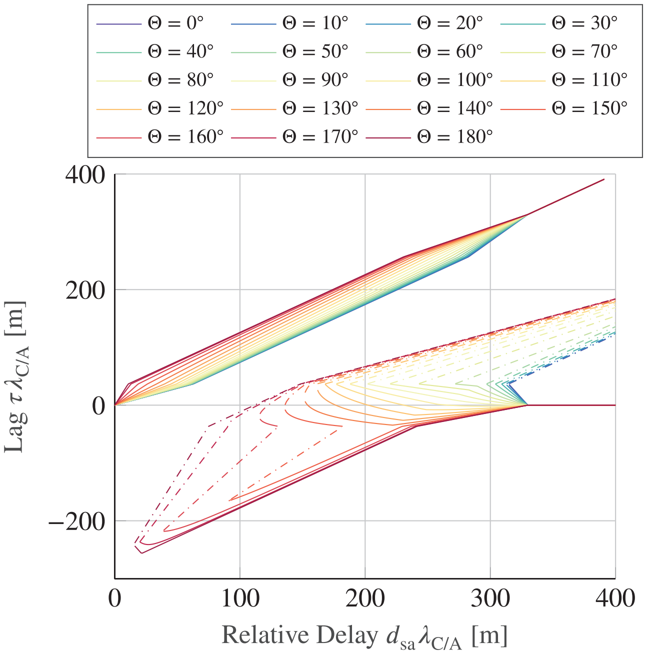


FIGURE 12 Lag values resulting in zero crossings of the S-curve as a function of the relative delay of the spoofing signal; calculated for Θ in a range from 0° to 180°, $d_c = 0.25$, $\alpha^2 = 2$, and $\Gamma = \frac{-1}{1023}$. The solid line marks a zero crossing with a negative slope (stable tracking points) and the dash-dotted line marks a zero crossing with a positive slope (unstable tracking points).

Figure 12 shows the stable and unstable tracking points for the same spoofing scenario as Figure 4, but for more relative phase values. As mentioned before, all stable tracking points should be taken into account in order to derive the generalized bound. The stable tracking point with the largest tracking bias defines the upper bound and the tracking point with the lowest bias defines the lower bound of the generalized tracking bound. By comparing Figure 12 with Figure 6, it can be observed that most parts of the SEE can be used to define the generalized bound because the SEE is defined by the stable tracking points with the largest/lowest tracking bias.

Considering the upper bound, it is helpful that parts of the SEE, Equation (9b) and Equation (9c), were chosen to be non-tight (see Section 5.2). Only the last line segment after the (upper) jump (Equation [9d]) must be redefined for the generalized bound. Remember: From the point of view of the spoofing signal, the authentic satellite signal affects the tracking like a multipath signal. Hence, we can reuse the multipath bounds of Braasch (1997) from the point of view of the spoofing signal for large delays and replace Equation (9d) with:

$$\tau_{\mathrm{Max}} = 1 + \alpha \frac{d_c}{2} \frac{\Gamma_{\max} - \Gamma_{\min}}{1 - \Gamma} \qquad \text{for} \quad d_{sa} > 1 + \frac{d_c}{2}\left[1 + \frac{\alpha\left(\Gamma_{\max} - \Gamma_{\min}\right)}{1 - \Gamma}\right] \tag{13}$$

For the lower bounds of the SEE, the two segments (Equation [10a] and Equation [10b]) before the (lower) jump of the SEE need to be redefined. The lowest stable tracking point in this area is defined by Equation (10c), but is only partly used for the bounds of the SEE. For the generalized bound, the range of the equation needs to be extended. For the sake of simplicity, we do not limit the extension as observed in Figure 12 but extend it until $\tau = 0$. Hence, (10c) replaces (10a) and (10b). The resulting equation reads:

$$\tau_{\mathrm{Min}} = d_{\mathrm{sa}} - 1 + \frac{d_{\mathrm{c}}}{\alpha} - \frac{d_{\mathrm{c}}}{2} \quad \text{for} \quad 0 < d_{\mathrm{sa}} \leq 1 - \frac{d_{\mathrm{c}}}{\alpha} \tag{14}$$

The remaining parts of the SEE can be directly taken for the generalized bound.

The generalized bound is plotted in Figure 13 for different correlator spacings d_{c}. The SEE is also plotted in the figure so that the common parts of the SEE and the generalized bound in the case of $d_{\mathrm{c}} = 0.1$ can be clearly recognized.

It can be observed that smaller correlator spacings lead to narrower bounds.

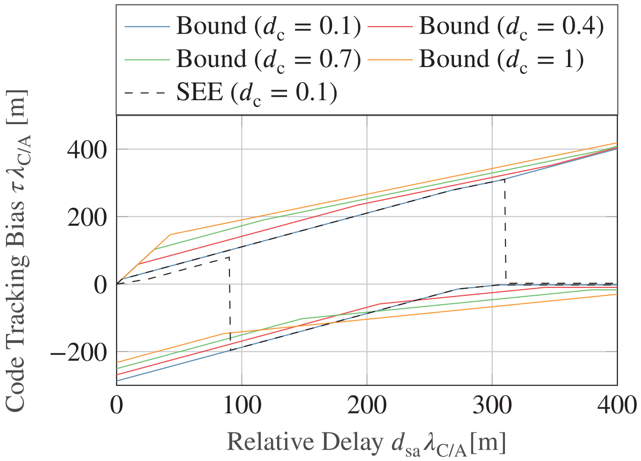


FIGURE 13 General tracking bound for d_{c} from 0.1 to 1 and $\alpha^2 = 2$. For comparison, the SEE is also plotted for $d_{\mathrm{c}} = 0.1$ To represent a worst-case error envelope for GPS L1 C/A, the following sidelobe levels were chosen to calculate the bounds: $\Gamma = \frac{-65}{1023}$, $\Gamma_{\mathrm{max}} = \frac{63}{1023}$, and $\Gamma_{\mathrm{min}} = \frac{-65}{1023}$.

8 | DISCUSSION OF THE APPLICATION OF INTRODUCED BOUNDS

In this work, we presented a method allowing us to compute the bounds of the tracking error of a receiver encountering a spoofing signal. The first bound, the Spoofer Error Envelope (SEE), gives a minimal and maximal (initial) tracking error for each parameter of the spoofing signal (relative delay, relative power, relative phase offset). We say *initial* here because the SEE assumes that, initially, the (authentic) satellite signal is tracked and that, at least, the relative delay of the spoofing signal remains constant. The second, more generalized bound even limits the tracking error without this assumption (i.e., the spoofer can arbitrarily change its signal parameters, but as soon as the DLL reaches a steady state, the corresponding tracking error limits are defined by this bound). The developed bounds can be used for these purposes:

1. The method used to derive these bounds allows for the development of a fundamental understanding of how a tracking loop is captured by a spoofing signal. This further gives a sense of the expected tracking error during a spoofing attack. Having this knowledge allows us the opportunity to design new receiver and signal structures that are more resilient against spoofing (new discriminators, new modulation schemes, etc.).

2. Furthermore, the method can be used to compare the effect of different receiver configurations, different discriminators, and different signal structures on the expected tracking error. Consequently, state-of-the-art receiver configurations can be adapted to reduce the effect of a spoofing signal, and, hence, be more resilient against spoofing attacks.
3. The bounds allow for the design of integrity monitors that can identify critical spoofing cases: A spoofing case, in the sense of delay/power combinations, is critical if the tracking error exceeds an alert limit. To design such a monitor, it is first necessary to analyze which spoofing cases must be detected with a high probability. The proposed method can be used to identify these cases for a given receiver design (discriminator, correlator spacing, etc.).

9 | CONCLUSION

In this paper, we presented a method to assess the effect of a spoofing signal on the tracking of an authentic satellite signal in terms of a code tracking bias. To demonstrate the method, we derived and proposed a Spoofer Error Envelope (SEE) for the widely-used non-coherent discriminator tracking the GPS L1 C/A signal. The SEE complements the methodology of the Multipath Error Envelope (MEE) described by Braasch (1997) and Van Nee (1992) to spoofing signals. While the MEE assumes that the additional signal (the multipath) is less powerful than the satellite signal (line-of-sight), the SEE is valid for additional signals that are more powerful than the satellite signal.

The proposed SEE is (like the MEE) independent of the relative phase between the additional signal and the satellite signal. Both envelopes are based on the expected tracking error of the in-phase and the counter-phase cases. To legitimatize this approach, we demonstrated that the aforementioned cases represent the worst-case regarding the tracking error. Parts of this demonstration are based on numerical results for highly relevant cases. These cases include different parameter settings, which are, for example, within the defined range of the MOPS as defined by RTCA SC-159 (2019). In addition, the SEE was verified by comparing it to results from signal tracking simulations using synthetically generated signals. A complete analytical proof is a challenge of future work.

In addition, we discussed the effect of a relative Doppler offset between the satellite and the spoofing signal on the SEE. In order to analyze the effect, we gave a short digression on the transition from the MEE to the SEE as a function of the additional-signal-to-satellite power ratio. Finally, we presented a generalized bound that can be used in dynamic spoofing scenarios to assess the tracking error development in the course of a spoofing attack.

The SEE allows us to assess the tracking error for spoofing signals as a function of the relative signal power, the relative signal delay, and the sidelobe level of the corresponding autocorrelation function as well as the correlator spacing of the early-late discriminator. Additionally, the methodology allows for an assessment of the tracking errors for arbitrary discriminator functions and even for new signal structures. Consequently, the assessment can not only be used to improve the receiver system, but also to develop new—more resilient—signal structures.

REFERENCES

Akos, D. M. (2012). Who's afraid of the spoofer? GPS/GNSS spoofing detection via automatic gain control (AGC). *NAVIGATION, 59*(4), 281–290. https://doi.org/10.1002/navi.19

Bamberg, T., Appel, M. M., & Meurer, M. (2018). Which GNSS tracking loop configuration is most robust against spoofing? *Proc. of the 31st International Technical Meeting of the Satellite*

Division of the Institute of Navigation (ION GNSS+ 2018), Miami, FL, 3587–3595. https://doi.org/10.33012/2018.15912

Braasch, M. S. (1992). *On the characterization of multipath errors in satellite-based precision approach and landing systems* [Doctoral dissertation]. Ohio University. https://www.proquest.com/openview/95cbc5d0bdac7aa5fa94ad9e5d47dcba/1?pq-origsite=gscholar&cbl=18750&diss=y

Braasch, M. S. (1997). Autocorrelation sidelobe considerations in the characterization of multipath errors. *IEEE Transactions on Aerospace and Electronic Systems*, *33*(1), 290–295. https://doi.org/10.1109/7.570787

Fernández-Hernández, I., Walter, T., Alexander, K., Clark, B., Châtre, E., Hegarty, C., Appel, M., & Meurer, M. (2019). Increasing international civil aviation resilience: A proposal for nomenclature, categorization and treatment of new interference threats. *Proc. of the 2019 International Technical Meeting of the Institute of Navigation,* Reston, VA. https://www.ion.org/publications/abstract.cfm?articleID=16699

Günther, C. (2014). A survey of spoofing and counter-measures. *NAVIGATION, 61*(3), 159–177. https://doi.org/10.1002/navi.65

Humphreys, T. E., Ledvina, B. M., Psiaki, M. L., O'Hanlon, B. W., & Kintner Jr, P. M. (2008). Assessing the spoofing threat: Development of a portable GPS civilian spoofer. *Proc. of the 21st International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2008),* Savannah, GA, 2314–2325. https://www.ion.org/publications/abstract.cfm?articleID=8132

Irsigler, M., Hein, G. W., & Eissfeller, B. (2004). Multipath performance analysis for future GNSS signals. *Proc. of the 2004 National Technical Meeting of the Institute of Navigation*, San Diego, CA, 225–238. Retrieved 2021-03-05, from https://www.ion.org/publications/abstract.cfm?articleID=5498

Kaplan, E. D., & Hegarty, C. J. (2005). *Understanding GPS: Principles and applications*. Artech House.

Kelly, J. M., Braasch, M. S., & DiBenedetto, M. F. (2003). Characterization of the effects of high multipath phase rates in GPS. *GPS Solutions*, *7*(1), 5–15. https://doi.org/10.1007/s10291-003-0043-9

Presti, L. L., & Motella, B. (2010). The math of ambiguity: What is the acquisition ambiguity function and how is it expressed mathematically? *Inside GNSS*. https://insidegnss.com/the-math-of-ambiguity

RTCA SC-159. (2019, June). *Minimum Operational Performance Standards for GPS local area augmentation system airborne equipment* (Technical Report DO-253D). RTCA. https://my.rtca.org/nc__store?search=253d

Teunissen, P. J. G., & Montenbruck, O. (Eds.). (2017). *Springer handbook of global navigation satellite systems*. Springer International Publishing. https://doi.org/10.1007/978-3-319-42928-1

Van Nee, R. D. J. (1992). Reducing multipath tracking errors in spread-spectrum ranging systems. *Electronics Letters*, *28*(8), 729–731. https://doi.org/10.1049/el:19920462

Van Nee, R. D. J. (1993). Spread-spectrum code and carrier synchronization errors caused by multipath and interference. *IEEE Transactions on Aerospace and Electronic Systems, 29*(4), 1359–1365. https://doi.org/10.1109/7.259541

How to cite this article: Bamberg, T., Konovaltsev, A., & Meurer, M. (2022) Developing a Spoofer Error Envelope for tracking GNSS signals. *NAVIGATION, 69*(3). https://doi.org/10.33012/navi.534

APPENDIX

A | PROOF OF BOUNDS

In this section, we show and give evidence that the Spoofer Error Envelope (SEE), as defined in Section 5.1, describes a bound of the tracking bias τ for all phase offsets Θ. Let $\tau_{\text{stp}}(d_{\text{sa}}, \Theta)$ be the stable tracking point that will be tracked according to the set of parameters and the assumption that the satellite is tracked before the spoofing signal is switched on. Mathematically, we want to show that:

$$\tau_{\text{stp}}(d_{\text{sa}}, \Theta) \leq \tau_{\text{SEEMax}}(d_{\text{sa}}) \tag{A1}$$

$$\tau_{\text{stp}}(d_{\text{sa}},\Theta) \geq \tau_{\text{SEEMin}}(d_{\text{sa}}) \tag{A2}$$

for all phase offsets $0° \leq \Theta < 360°$ and all positive signal delays $0 < d_{\text{sa}}$.

As described in Section 3.2 and Section 5.1, we postulate:

$$0 < d_{\text{c}} \leq 1 \tag{A3a}$$

$$1 < \alpha \leq \frac{1-\Gamma}{\Gamma_{\max} - \Gamma_{\min}} \tag{A3b}$$

$$-1 < \Gamma < 1 \tag{A3c}$$

A.1 | Zones

To proof the bounds, we analyze the envelope separately for three zones with respect to d_{sa}, depending on the sign of the discriminator value at $\tau = 0$. These zones are visualized for an exemplary SEE in Figure A1.

Zone 1 In the first zone ($0 < d_{\text{sa}} < d_{\text{sa,jump}}$), the discriminator output at $\tau = 0$ is positive for all Θ, i.e., $D(\tau = 0) > 0$. Due to the mechanism of the DLL (see Section 3.3), the replica will be delayed until it reaches a stable tracking point (i.e., $\tau_{\text{stp}} > 0$). Only the upper stable tracking point needs to be considered.

Zone 2 In the second zone ($d_{\text{sa,jump}} \leq d_{\text{sa}} < 1 + \frac{d_{\text{c}}}{2}$), the discriminator output at $\tau = 0$ depends on Θ. Both upper ($\tau_{\text{stp}} > 0$, delayed replica) and lower ($\tau_{\text{stp}} < 0$, advanced replica) stable tracking points need to be considered.

Zone 3 In the third zone ($1 + \frac{d_{\text{c}}}{2} \leq d_{\text{sa}}$), the discriminator output at $\tau = 0$ is always zero. This is readily shown by solving $D(\tau = 0) = 0$ for $d_{\text{sa}} > 1 + \frac{d_{\text{c}}}{2}$. However, for the SEE, we used the tracking bias estimation of Braasch (1997) to account for changing sidelobe levels.

In the next step, we will focus on the border between Zone 1 and Zone 2. This is split into three sections:

1. We show that Zone 1 always exists, i.e., there is a $d_{\text{sa,jump}} > 0$ so that $D(\tau = 0) > 0$ for $0 < d_{\text{sa}} < d_{\text{sa,jump}}$.

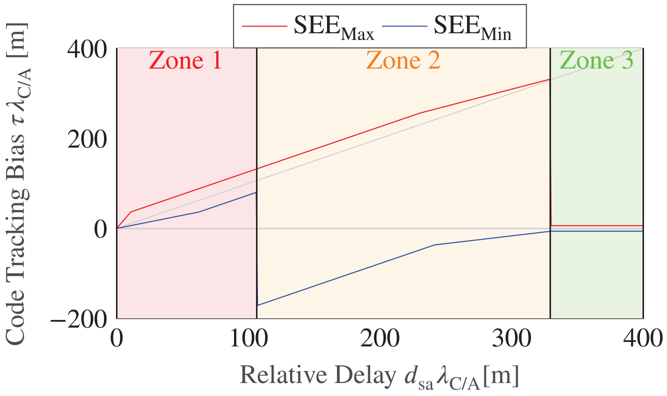


FIGURE A1 Exemplary visualization of the defined zones; for this example, a Spoofer Error Envelope with $d_{\text{c}} = 0.25$, $\alpha^2 = 2$, $\Gamma = \frac{-65}{1023}$, $\Gamma_{\max} = \frac{63}{1023}$, and $\Gamma_{\min} = \frac{-65}{1023}$ was plotted.

2. We determine potential upper limits of Zone 1 with respect to the relative phase Θ.
3. In order to ensure that we have $D(\tau=0)>0$ in Zone 1 for all phases Θ, we determine the lowest of the potential upper limits to define the upper limit of Zone 1 $(d_{\mathrm{sa,jump}})$.

A.1.1 | *Zone 1 Always Exists*

Evaluating Equation (6) together with Equation (7), some algebraic manipulations of $D(\tau=0)>0$ under the assumption $0<d_{\mathrm{sa}}<\frac{d_{\mathrm{c}}}{2}$ yield:

$$\underbrace{4d_{\mathrm{sa}}(1-\Gamma)}_{\substack{>0\\ \text{for}\\ d_{\mathrm{sa}}>0 \text{ and } \Gamma<1}}\underbrace{\left[1+(\Gamma-1)\frac{d_{\mathrm{c}}}{2}\right]}_{\substack{>0\\ \text{for}\\ 0<d_{\mathrm{c}}\leq 1 \text{ and } \Gamma>-1}}\underbrace{\left[\alpha+\cos(\Theta)\right]}_{\substack{>0\\ \text{for}\\ \alpha>1}}>0 \tag{A4}$$

As indicated, this is true for all parameters within the predefined range (A3). Hence, Zone 1 always exists and spans at least the range $0<d_{\mathrm{sa}}<\frac{d_{\mathrm{c}}}{2}$.

A.2 | Potential Upper Limits of Zone 1

The discriminator function D as shown in Equation (6) is continuous because of the approximation of the autocorrelation function in Equation (7), the applied operations and the composed absolute value function are continuous. (The autocorrelation function is a piecewise-defined sequence of straight lines and there is no discontinuity at the endpoints of the subdomains.) Due to the continuity of the discriminator function D and (A4), we can conclude that the upper limit of Zone 1 is given by a root of the discriminator function at $\tau=0$.

Solving $D(\tau=0)=0$ (Equation [6] and Equation [7]) under the assumptions defined in Equation (A3) and within the range $\frac{d_{\mathrm{c}}}{2}\leq d_{\mathrm{sa}}<1+\frac{d_{\mathrm{c}}}{2}$ yields:

$$d_{\mathrm{sa}}(\Theta)=\begin{cases}\dfrac{\cos(\Theta)}{\alpha}\left(\dfrac{1}{1-\Gamma}-\dfrac{d_c}{2}\right)+\dfrac{1}{1-\Gamma} & \dfrac{\Gamma+\frac{d_{\mathrm{c}}}{2}(1-\Gamma)}{1-\frac{d_{\mathrm{c}}}{2}(1-\Gamma)}\leq\dfrac{-\cos(\Theta)}{\alpha}<1 \qquad \text{(A5a)}\\[2ex] \dfrac{2\cos(\Theta)}{\alpha}\left(\dfrac{1}{1-\Gamma}-\dfrac{d_c}{2}\right)+\dfrac{1+\Gamma}{1-\Gamma}+\dfrac{d_{\mathrm{c}}}{2} & \dfrac{\Gamma}{1-\frac{d_{\mathrm{c}}}{2}(1-\Gamma)}<\dfrac{-\cos(\Theta)}{\alpha}<\dfrac{\Gamma+\frac{d_{\mathrm{c}}}{2}(1-\Gamma)}{1-\frac{d_{\mathrm{c}}}{2}(1-\Gamma)} \qquad \text{(A5b)}\end{cases}$$

To determine if the equation $D(\tau=0)=0$ has a solution, we focus on the subdomains of Equation (A5). Within the postulated assumption of Equation (A3), the upper bound of Equation (A5a), $\frac{-\cos(\Theta)}{\alpha}<1$, is always true. Hence, we only need to evaluate the lower bound of Equation (A5b):

$$\frac{\Gamma}{1-\frac{d_{\mathrm{c}}}{2}\left(1-\Gamma\right)}<\frac{-\cos(\Theta)}{\alpha}. \tag{A6}$$

If this condition is fulfilled, $D(\tau = 0) = 0$ has a solution within the range $0 < d_{\text{sa}} < 1 + \frac{d_{\text{c}}}{2}$. If not, Equation (A5) is not defined and the next zero of $D(\tau = 0)$ (with respect to d_{sa}) is given at $d_{\text{sa}} = 1 + \frac{d_{\text{c}}}{2}$. (Remember that $D(\tau = 0) = 0$ is always fulfilled for $d_{\text{sa}} \geq 1 + \frac{d_{\text{c}}}{2}$.) This means that, for some Θ, the discriminator output at zero is always greater or equal to zero $(D(\tau = 0) \geq 0)$, i.e., only the upper stable tracking point needs to be considered for these phases. To get a better feeling for this condition it is helpful to set the sidelobe level to zero, i.e., $\Gamma = 0$. Then Equation (A6) becomes:

$$0 < \frac{-\cos(\Theta)}{\alpha}. \tag{A7}$$

In this special case, a lower stable tracking point $(\tau_{\text{stp}} < 0)$ needs to be considered for $90° < \Theta < 270°$. For all other phases, only the upper stable tracking point $(\tau_{\text{stp}} \geq 0)$ needs to be considered.

A.2.1 | The Upper Limit of Zone 1

Zone 1 is supposed to span the range of d_{sa}, where all phase offsets Θ result in a positive discriminator output. Therefore, we need to find the smallest delay, d_{sa}, defined by Equation (A5) that yield a root of the discriminator function for $d_{\text{sa}} > 0$ over all phase offsets:

$$d_{\text{sa,jump}} = \min_{0° \leq \Theta < 360°} d_{\text{sa}}(\Theta) \tag{A8}$$

Note, that this delay also gives the earliest jump of the SEE over all phases Θ (see Section 4.1).

Basically, both sub-functions of Equation (A5) are a product of the cosine function with a factor and a subsequent addition. The factor is positive, i.e., $\left(\frac{1}{1-\Gamma} - \frac{d_{\text{c}}}{2}\right) > 0$, for the postulated ranges $d_{\text{c}} \leq 1$ and $|\Gamma| < 1$). Hence, within the range $0° \leq \Theta < 360°$, both sub-functions have a global maximum at $\Theta = 0°$ (in-phase case) and a global minimum at $\Theta = 180°$ (counter-phase case)

We now know the global minimum of the individual functions of the subdomains without considering its limits. Looking at Equation (A6) shows us that if Equation (A5) is defined for any phase, then it is also defined for $\Theta = 180°$. Furthermore, it is straightforward to show that the sub-function (A5a) is smaller than (A5b) within the subdomain of Equation (A5b):

$$\frac{\cos(\Theta)}{\alpha}\left(\frac{1}{1-\Gamma} - \frac{d_{\text{c}}}{2}\right) + \frac{1}{1-\Gamma} \tag{A9}$$

$$< \frac{2\cos(\Theta)}{\alpha}\left(\frac{1}{1-\Gamma} - \frac{d_{\text{c}}}{2}\right) + \frac{1+\Gamma}{1-\Gamma} + \frac{d_{\text{c}}}{2}$$

$$\Longleftrightarrow \frac{-\cos(\Theta)}{\alpha} < \frac{\Gamma + \frac{d_{\text{c}}}{2}(1-\Gamma)}{1 - \frac{d_{\text{c}}}{2}(1-\Gamma)} \tag{A10}$$

Equation (A10) is the same as the upper limit of the subdomain (A5b) and, hence, if we are in the subdomain of Equation (A5b) and if Equation (A5) is defined, this statement is true.

A.2.2 | Summary

Summing up, we now have the following statements:

1. For $0 < d_{\mathrm{sa}} < \frac{d_{\mathrm{c}}}{2}$, we have $D(\tau = 0) > 0$.
2. The function of D is continuous and, in the range $\frac{d_{\mathrm{c}}}{2} \leq d_{\mathrm{sa}} < 1 + \frac{d_{\mathrm{c}}}{2}$, we have a zero of D at $d_{\mathrm{sa}}(\Theta)$ as described by Equation (A5).
3. The functions of the two subdomains of $d_{\mathrm{sa}}(\Theta)$, Equation (A5), have a global maximum at $\Theta = 0°$ and a global minimum at $\Theta = 180°$.
4. The sub-function (A5a) is smaller than the sub-function (A5b) in the subdomain of Equation (A5b).
5. If Equation (A5) is defined for an arbitrary phase Θ, it is always defined for $\Theta = 180°$.

Putting all the information together, we can use Equation (A5a) to define the upper limit of Zone 1. We have shown that a relative delay d_{sa} greater than zero but smaller than:

$$d_{\mathrm{sa,jump}} = \frac{1}{1-\Gamma} - \frac{1}{\alpha}\left(\frac{1}{1-\Gamma} - \frac{d_{\mathrm{c}}}{2}\right) \tag{A11}$$

The discriminator output at zero is always positive, i.e., $D(\tau = 0) > 0$.

A.3 | Bounds of the Tracking Bias Over all Phases

In the previous section, we defined three zones with respect to d_{sa}. In this section, we will show for each zone individually that the stable tracking point τ_{stp} used for the SEE defined by Equation (10) and Equation (9) describes a bound over all phase Θ.

To get a better understanding of τ_{stp}, Figure A2 displays the numerically calculated code tracking bias of stable tracking points as a function of the phase. The figure is separated into eight subfigures representing different parameter sets of the relative power α and the correlator spacing d_{c}. In each subfigure, the relevant stable tracking point τ_{stp} is plotted as a bold line for different delays d_{sa}. Non-relevant stable tracking points are plotted as dashed lines. *Relevant* here means that this stable tracking point is tracked due to the mechanism of the DLL evaluating the discriminator output at $\tau = 0$.

A.3.1 | Zone 1

Looking at the delay of 50 m (blue line), which is smaller than $d_{\mathrm{sa,jump}}$ for all displayed parameter sets, confirms the statement for Zone 1: Only the upper stable tracking point is relevant. In some subfigures, an additional lower stable tracking point is shown. However, it is never relevant as indicated by the dashed line. The same applies to the red line (150 m) of the higher relative power $\alpha^2 = 8$ and in the bottom-left subfigure ($\alpha^2 = 2$, $d_{\mathrm{c}} = 1.0$) as well as for the green line in the bottom-right subfigure ($\alpha^2 = 8$, $d_{\mathrm{c}} = 1.0$). These plots still belong to Zone 1, as the upper limit of Zone 1 shifts to a higher relative delay d_{sa} for higher relative powers and larger correlator spacings.

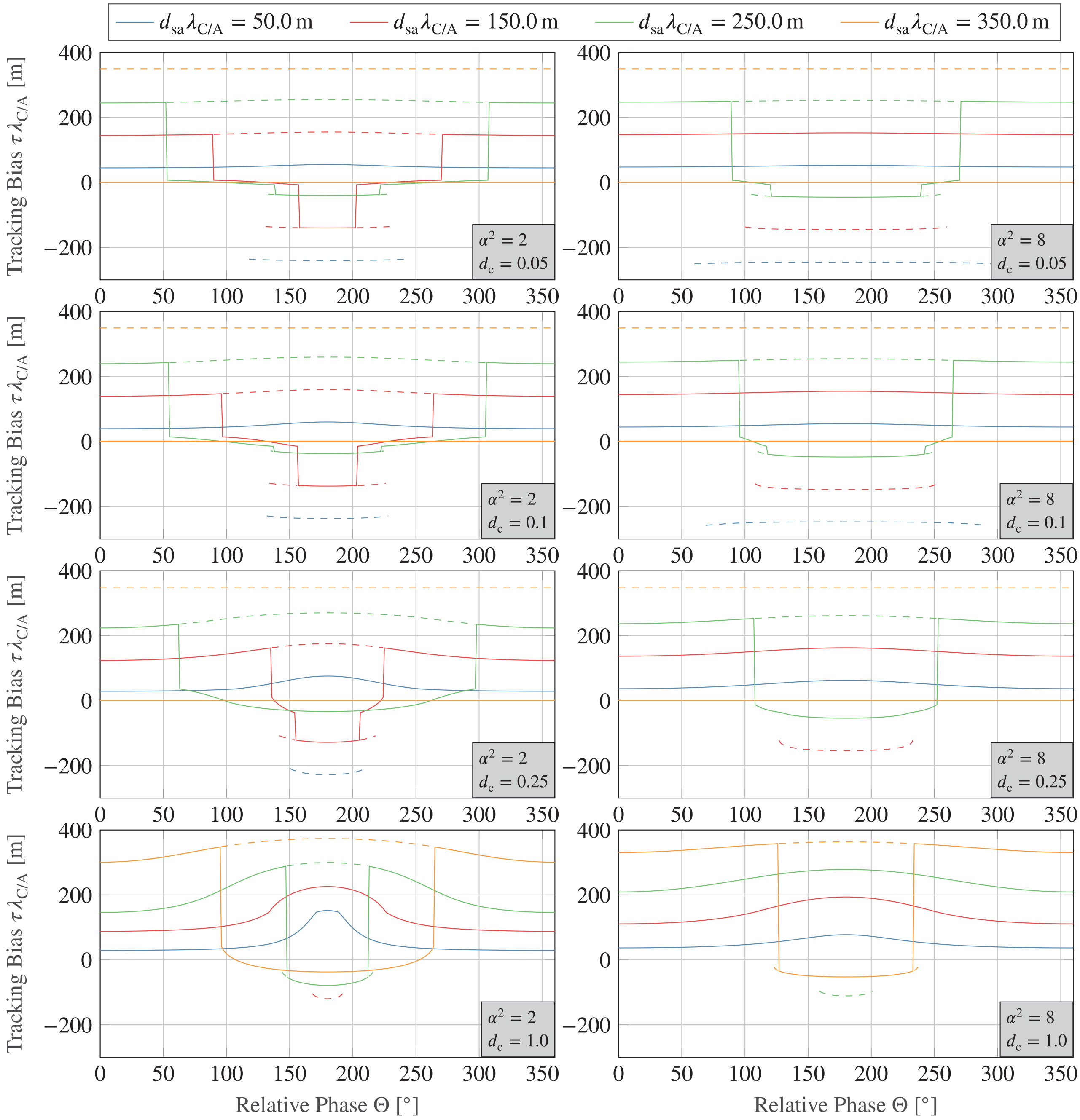


FIGURE A2 Numerically calculated (relevant) stable tracking point τ_{stp} as a function of the phase Θ for different delays d_{sa} (bold line); the dashed line marks a stable tracking point that is not tracked due to the sign of the discriminator function at $\tau = 0$. In this figure, the correlator spacing d_c ranges from 0.05 to 1.0 and the relative power α from 2 to 8. For the calculation, a (constant) sidelobe level of $\Gamma = \frac{-65}{1023}$ was assumed.

The plots indicate that there is a minimum of the upper stable tracking point for $\Theta = 0°$ and a maximum for $\Theta = 180°$. The exact phases of the extrema can not be read from the plots. However, the proof that the derivative of a stable tracking with respect to the phase is zero at these points is supported by Appendix B. Furthermore, the problem of solving for the upper stable tracking points can be transferred to a multipath scenario and the extrema are then given by the MEE. For the dual-problem, we define the spoofing signal as the satellite signal and the (original) satellite signal as the multipath signal. The MEE can be considered because:

1. We postulated that the spoofing signal has higher power than the satellite signal ($\alpha > 1$). Hence, the newly defined multipath signal is weaker than the newly defined satellite signal (i.e., $\alpha' := \frac{1}{\alpha} < 1$).
2. We postulated a delayed spoofing signal compared to the satellite signal ($d_{\mathrm{sa}} > 0$). Hence, the newly defined multipath signal is advanced compared to the newly defined satellite signal (i.e., $d'_{\mathrm{sa}} = -d_{\mathrm{sa}} < 0$). The MEE is usually only defined for positive delays because a multipath signal is always a delayed replica of the line-of-sight signal. However, due to the symmetry of the autocorrelation function, the discriminator function is odd symmetric $D(\tau, d_{\mathrm{sa}}) = -D(-\tau, -d_{\mathrm{sa}})$. Hence, the function of the MEE can be continued in the negative domain of d_{sa} as an odd function.

It is well known that the in-phase case $(\Theta = 0°)$ poses an upper bound of the tracking bias in the multipath scenario over all phases as well as the counter-phase case $(\Theta = 180°)$ poses a lower bound (Braasch, 1997; Van Nee, 1992). Due to the odd symmetry, the upper bound of a negative delay d_{sa} becomes a lower bound and vice-versa. Back to the SEE, we can now say that the counter-phase case is an upper and the in-phase case a lower bound of the (upper) stable tracking point.

A.3.2 | *Zone 2*

In Figure A2 the following graphs belong to Zone 2:

- The remaining red plots (150 m) that are not listed in the previous section; these are in the top three left subfigures ($\alpha^2 = 2$ and $d_{\mathrm{c}} \in \{0.05, 0.1, 0.25\}$).
- All green plots (250 m) except of the one in the bottom right subfigure $(\alpha^2 = 8,$ $d_{\mathrm{c}} = 1.0)$
- The orange plots (350 m) in the bottom subfigures ($d_{\mathrm{c}} = 1.0$)

In Zone 2, the situation is more complicated than in Zone 1: Depending on the parameter set, we have up to four jumps (as it is an even function with two jumps on each side). For a correlator spacing of $d_{\mathrm{c}} = 0.25$ and, in the bottom-left plot, the green line shows two jumps. In all remaining graphs four jumps can be observed.

We can use the same reasoning as for Zone 1 to show that the counter-phase case $(\Theta = 180°)$ poses an upper bound. Even though the bound is not always reached—as the relevant stable tracking point switches to a lower one for a range around $\Theta = 180°$—it is still a valid stable tracking point and, therefore, limits the tracking bias. Remember, the presence of a stable tracking point is indicated by a dashed line in the plots.

For the lower bound, we need to consider the lower stable tracking points $(\tau < 0)$. As indicated by the jumps in the course, there are up to two different lower stable tracking points. One lies around zero and is defined for two ranges (excluding a range around $\Theta = 180°$). The second one lies lower and is defined exclusively for a range around $\Theta = 180°$. The latter is needed for a bound that is lower than the former. The graph indicates that the lower stable tracking point is a continuous and differentiable function including a minimum at $\Theta = 180°$. Hence, applying Appendix B gives strong evidence for a minimum at $\Theta = 180°$ for the lower stable tracking point.

Summing up, for Zone 2 the in-phase case of the upper stable tracking point gives an upper bound and the in-phase case of the lower stable tracking point gives a lower bound.

A.3.3 | Zone 3

For most of the displayed parameter settings in Figure A2, a relative delay of 350 m (orange line) belongs to Zone 3 (all except the two bottom subfigures with a correlator spacing of $d_c = 1.0$). As already mentioned and confirmed in the plots, finding zeros of $D(\tau)$ for relative delays, $d_{sa} \geq 1 + \frac{d_c}{2}$, lead to a constant solution at $\tau = 0$ over all phases Θ. The reason for this solution is that the autocorrelation function is approximated using a constant sidelobe level; see Equation (7). However, Braasch (1997) derived a lower/upper limit of:

$$\tau = \frac{\pm \alpha d_c \left(\Gamma_{\max} - \Gamma_{\min}\right)}{2(1 - \Gamma)} \tag{A12}$$

by considering the maximal and minimal slope between two adjacent sidelobe levels of the autocorrelation function $\Gamma_{\max} - \Gamma_{\min}$. The derived limits apply for:

$$\alpha \leq \frac{1 - \Gamma}{\Gamma_{\max} - \Gamma_{\min}} \tag{A13}$$

which was postulated in Equation (A3).

B | CHARACTERISTICS OF THE IN-PHASE AND COUNTER-PHASE REGARDING TRACKING BIAS

In this section, we want to give evidence that the in-phase $\Theta = 0°$ and the counter-phase $\Theta = 180°$ cases give (local) extrema regarding the tracking bias. We assume there are continuous and differentiable functions $\tau_{\text{stp},k}(\Theta)$ describing the stable tracking point k (some parameter sets yield more than one solution) as a function of the relative carrier phase. It is challenging to give an explicit solution for all $\tau_{\text{stp},k}(\Theta)$. Therefore, we shall confine ourselves to show that the derivation of these functions is zero for the in-phase and the counter-phase case.

Mathematically, we want to show that:

$$\left(\frac{\partial \tau_{\text{stp},k}}{\partial \Theta}\right)_{\Theta = 0°} = 0 \quad \text{and} \quad \left(\frac{\partial \tau_{\text{stp},k}}{\partial \Theta}\right)_{\Theta = 180°} = 0 \tag{B1}$$

To get the derivative without solving the explicit form, we use a method called implicit differentiation. The approach can be described by the following steps:

1. Calculate the implicit differentiation and rearrange the equation to give the derivative of $\tau_{\text{stp},k}(\Theta)$ (the derivative will be given by a fraction).
2. Show that the nominator of the derivative is zero for the in-phase and the counter-phase cases.
3. Show that the denominator of the derivative is non-zero for the in-phase and the counter-phase cases.

B.1 | Calculate the Implicit Differentiation

By definition, the functions $\tau_{\mathrm{stp},k}(\Theta)$ give stable tracking points:

$$D(\tau_{\mathrm{stp},k}(\Theta),\Theta)=0 \tag{B2}$$

Using the method of the implicit differentiation yields:

$$\frac{\mathrm{d}D\left(\tau_{\mathrm{stp},k}(\Theta),\Theta\right)}{\mathrm{d}\Theta}=\frac{\partial D}{\partial\Theta}+\frac{\partial D}{\partial\tau}\frac{\partial\tau_{\mathrm{stp},k}}{\partial\Theta}=0 \tag{B3}$$

For $\frac{\partial D}{\partial\tau}\left(\tau_{\mathrm{stp},k}(\Theta),\Theta\right)\neq 0,$ we get:

$$\frac{\partial\tau_{\mathrm{stp},k}(\Theta)}{\partial\Theta}=-\frac{\frac{\partial D}{\partial\Theta}\left(\tau_{\mathrm{stp},k}(\Theta),\Theta\right)}{\frac{\partial D}{\partial\tau}\left(\tau_{\mathrm{stp},k}(\Theta),\Theta\right)} \tag{B4}$$

B.2 | Show That the Nominator of the Derivative is Zero for the In-Phase and the Counter-Phase Cases

The partial derivative of the S-Curve given by Equation (6) with respect to Θ reads:

$$\frac{\partial D}{\partial\Theta}(\tau,\Theta)=\alpha\sin(\Theta)\left(\frac{R\left(\tau-\frac{d_\mathrm{c}}{2}\right)R\left(\tau-\frac{d_\mathrm{c}}{2}-d_\mathrm{sa}\right)}{\left|R\left(\tau-\frac{d_\mathrm{c}}{2}\right)+\alpha R\left(\tau-\frac{d_\mathrm{c}}{2}-d_\mathrm{sa}\right)e^{\mathrm{j}\Theta}\right|}-\frac{R\left(\tau+\frac{d_\mathrm{c}}{2}\right)R\left(\tau+\frac{d_\mathrm{c}}{2}-d_\mathrm{sa}\right)}{\left|R\left(\tau+\frac{d_\mathrm{c}}{2}\right)+\alpha R\left(\tau+\frac{d_\mathrm{c}}{2}-d_\mathrm{sa}\right)e^{\mathrm{j}\Theta}\right|}\right) \tag{B5}$$

For the in-phase and for the counter-phase, one can show by setting $\Theta=0^\circ$ and $\Theta=180^\circ$ that this partial derivative is zero:

$$\left(\frac{\partial D}{\partial\Theta}\right)_{\Theta=0^\circ}=0 \quad \text{and} \quad \left(\frac{\partial D}{\partial\Theta}\right)_{\Theta=180^\circ}=0 \tag{B6}$$

With this information and Equation (B4), we know that:

$$\left(\frac{\partial\tau_{\mathrm{stp},k}(\Theta)}{\partial\Theta}\right)_{\Theta=0^\circ}=0 \quad \text{for} \quad \frac{\partial D}{\partial\tau}\left(\tau_{\mathrm{stp},k}(0^\circ),0^\circ\right)\neq 0 \tag{B7}$$

and:

$$\left(\frac{\partial\tau_{\mathrm{stp},k}(\Theta)}{\partial\Theta}\right)_{\Theta=180^\circ}=0 \quad \text{for} \quad \frac{\partial D}{\partial\tau}\left(\tau_{\mathrm{stp},k}(180^\circ),180^\circ\right)\neq 0 \tag{B8}$$

B.3 | Show That the Denominator of the Derivative is Non-Zero for the In-Phase and the Counter-Phase Cases

An explicit form of the denominator of Equation (B4) is not available in general. Therefore, we want to demonstrate that this term is only zero for a specific and limited amount of values of Θ.

For the in-phase and the counter-phase case, Equation (6) becomes:

$$D_{\mathrm{i/c}}(\tau)=\left|R\left(\tau+\frac{d_{\mathrm{c}}}{2}\right)+\alpha_{\mathrm{pm}}R\left(\tau+\frac{d_{\mathrm{c}}}{2}-d_{\mathrm{sa}}\right)\right| \\ -\left|R\left(\tau-\frac{d_{\mathrm{c}}}{2}\right)+\alpha_{\mathrm{pm}}R\left(\tau-\frac{d_{\mathrm{c}}}{2}-d_{\mathrm{sa}}\right)\right| \tag{B9}$$

with $\alpha_{\mathrm{pm}}=\alpha$ for the in-phase and $\alpha_{\mathrm{pm}}=-\alpha$ for the counter-phase case, respectively.

To get a better understanding of Equation (B9), we define:

$$R_{\alpha_{\mathrm{pm}}}(x):=R(x)+\alpha_{\mathrm{pm}}R\left(x-d_{\mathrm{sa}}\right) \tag{B10}$$

With this, Equation (B9) becomes:

$$D_{\mathrm{i/c}}(\tau)=\left|R_{\alpha_{\mathrm{pm}}}\left(\tau+\frac{d_{\mathrm{c}}}{2}\right)\right|-\left|R_{\alpha_{\mathrm{pm}}}\left(\tau-\frac{d_{\mathrm{c}}}{2}\right)\right| \tag{B11}$$

Considering the approximation of the autocorrelation function $R(.)$ given by Equation (7), it becomes quite obvious that $R_{\alpha_{\mathrm{pm}}}(x)$ is a piecewise-defined sequence of straight lines: $R(.)$ is a piecewise-defined sequence of straight lines by definition and the linear combination of two lines is, again, a line. The same goes for the S-curve $D_{\mathrm{i/c}}$. The examples in Figure 1 and Figure 3 in the main text may illustrate the resulting S-curve. Additionally, the S-curve $D_{\mathrm{i/c}}$ is continuous due to the continuity of the autocorrelation function $R(.)$ and the continuity of the applied operations. However, they are only differentiable with respect to τ within one line segment and not at the corners. Summed up, the S-curve $D_{\mathrm{i/c}}$ is a continuous function of line segments.

Hence, the derivative of the S-curve with respect to τ is zero if and only if the S-curve has a horizontal line segment (i.e., a line segment with a slope of zero). A horizontal line segment of the S-curve is only given if the positions $\tau+\frac{d_{\mathrm{c}}}{2}$ and $\tau-\frac{d_{\mathrm{c}}}{2}$ are within one line segment of the summed autocorrelation function $R_{\alpha_{\mathrm{pm}}}(x)$ or within two line segments with the same slope. This can again be retraced in the shown examples (Figure 1 and Figure 3).

By the definition of $\tau_{\mathrm{stp},k}(\Theta)$, it must hold that $D\left(\tau_{\mathrm{stp},k}(\Theta),\Theta\right)=0$. Hence, the aforementioned horizontal line segment of the S-curve must be zero and the positions $\tau+\frac{d_{\mathrm{c}}}{2}$ and $\tau-\frac{d_{\mathrm{c}}}{2}$ must be within one horizontal line segment of the summed autocorrelation function $R_{\alpha_{\mathrm{pm}}}(x)$ or within two line segments with the same slope and same level. The summed autocorrelation function, again, is a linear combination of two autocorrelation functions that are constant except for an isosceles-triangular-shaped part—compare to Equation (7).

The linear combination yields a horizontal line segment only if:

1. The flanks of the triangular shapes of the two functions have the same (absolute) slope; we can neglect this case because it is only given for $\left|\alpha_{\mathrm{pm}}\right|=1$ but we presumed $\alpha>1$.
2. We consider a position outside of the triangular shapes of both functions; this position is not of interest because we start from the center of one triangular (the satellite is tracked before spoofing) and another stable tracking point will be reached first.

With this reasoning, it can be said that the denominator in Equation (B4) is (in general) not zero at the locations of stable tracking points and therefore:

$$\left(\frac{\partial\tau_{\mathrm{stp},k}}{\partial\Theta}\right)_{\Theta=0^\circ}=0 \qquad \text{and} \qquad \left(\frac{\partial\tau_{\mathrm{stp},k}}{\partial\Theta}\right)_{\Theta=180^\circ}=0 \tag{B12}$$

hold for all relevant positions. Hence, the in-phase and the counter-phase cases give extrema or saddle points regarding the tracking error.