Which GNSS tracking loop configuration is most robust against spoofing?

Tobias Bamberg*†, Manuel M. Appel*†, Michael Meurer *†
* *Institute of Communications and Navigation, German Aerospace Center (DLR), Oberpfaffenhofen, Germany*
† *Chair of Navigation, RWTH Aachen University, Germany*
Email: tobias.bamberg@dlr.de

BIOGRAPHY

Tobias Bamberg received his M.Sc. in electrical engineering from RWTH Aachen University in 2017. He completed his Master thesis in the field of GNSS spoofing detection and mitigation. In November 2017 he joined the Institute of Communications and Navigation of the German Aerospace Center (DLR) in Oberpfaffenhofen and began his doctorate studies at RWTH Aachen University. His main research interest lies on the development of robust and precise multi-antenna GNSS receivers focused on the signal processing layer.

Manuel M. Appel received his diploma degree (FH) in electrical engineering from Technical University Ingolstadt, Germany in 2008. In 2009 he joined Fraunhofer Institute for Integrated Circuits ("home of mp3") in Erlangen. From 2010 until 2012 he was with the Center of Applied Research in Ingolstadt, focusing on forward looking safety systems for the automotive industry. During that time, he was involved in the conception and planning of the center of automotive research and testing (Carissma). Partly in parallel, he received a M.Sc. degree from Technical University Munich in 2013.
He joined the Institute for Communication and Navigation of DLR in January 2014. His main research interest lies in development of signal processing algorithms for robust GNSS receivers with the main focus on spoofing detection and mitigation. In addition, he focuses on drone capturing using spoofing. This enables him to finish his doctoral studies at RWTH Aachen.

Michael Meurer received the diploma in electrical engineering and the Ph.D. degree from the University of Kaiserslautern, Germany. After graduation, he joined the Research Group for Radio Communications at the Technical University of Kaiserslautern, Germany, as a senior key researcher, where he was involved in various international and national projects in the field of communications and navigation both as project coordinator and as technical contributor. From 2003 till 2013, Dr. Meurer was active as a senior lecturer and Associate Professor (PD) at the same university. Since 2006 Dr. Meurer is with the German Aerospace Centre (DLR), Institute of Communications and Navigation, where he is the director of the Department of Navigation and of the center of excellence for satellite navigation. In addition, since 2013 he is a professor of electrical engineering and director of the Chair of Navigation at the RWTH Aachen University. His current research interests include GNSS signals, GNSS receivers, interference and spoofing mitigation and navigation for safety-critical applications.

ABSTRACT

The use of GNSS positioning in highly automated systems, like packet delivering using drones or self-driving cars, demands a reliable position estimation. One major risk to the position estimation is the so called spoofing threat. A spoofer fakes satellite signals in order to mislead a GNSS receiver into estimating a wrong user position. A lot of research focuses on the detection and mitigation of spoofing by evaluating several metrics implemented in the receiver. However, beforehand it should be investigated under which conditions a receiver is affected by spoofing. In this work a simulation tool is described to simulate a scenario, where a receiver structure processes a signal containing an authentic and a spoofing signal. The parameters of the spoofing signal are variated. These simulations are repeated with different receiver settings in order to evaluate robust configurations for GNSS receivers. The results show that especially the coherent integration time in the receiver's tracking loops has a large impact on the vulnerability of the receiver.

INTRODUCTION

Global navigation satellite systems (GNSS) are widely used for positioning and timing. The systems are used by almost every land, air and water vessel to help navigate or to navigate. The increasing number of private and commercial UAVs and the upcoming of autonomous driving cars will even increase the number of systems relying on GNSS. Therefore, it is getting more and more important to secure the reliability of the obtained position, velocity and time (PVT) solution. A state of the art GNSS receiver can be easily deceived by using a technique called spoofing [1]. A spoofer transmits replicas

of satellite signals to control a victim receiver's PVT estimate. In contrast to jamming, where the receiver's operation is significantly distorted, a spoofing attack may be undetected by the user, especially if the affected PVT solution is only slowly diverging over time. Hence, the detection of spoofing attacks is a major field of research. Several definitions and taxonomies of the different spoofing types have been provided in the literature. [2] provides a broader overview, especially also including different injection techniques of the spoofing signals into the victim receiver's input. However, synchronization aspects are not explicitly handled. A more detailed treatment and taxonomy of different spoofing and interference categories can be found in [3, Chapter 16]. Especially [1] provides a classification into simplistic, intermediate and sophisticated. The paper at hand will directly focus on the code synchronous (i.e. intermediate) type.

There are different approaches available in the literature to detect such a spoofing attack. The effectiveness of the detections highly depends on the stage of development of the spoofer. Psiaki et al [4] collected different strategies to detect spoofing and listed their limitations. However, he states that there is still a lot of research to do on detection and especially on mitigation. One advanced way to detect and mitigate a spoofer is using an antenna array and applying spatial filtering to the signal [5] [6] [7]. In these approaches the directions of arrival (DoA) of the satellite signals are estimated and compared to the expected ones extracted from the almanac and ephemeris. In [8] different metrics are described and compared. After spoofing detection the malicious signal can be mitigated by steering a spatial zero into its direction.

To improve detection and mitigation it is important to understand the effects of spoofing on a GNSS receiver. Typically, investigations focus on the effect of spoofing on the pseudorange, position estimation and SNR, like [9] for instance. These metrics are a direct or indirect result of the behavior of the receiver's tracking loops. To study the problem into more detail, the signal processing layer has to be taken into account. Kerns et al [10] did some research on the effect of a spoofing signal on tracking loops, but in his research the variation of the receiver tracking parameter was limited to the order of the loop filter and its bandwidth. Furthermore the effect of spoofing on the DLL and PLL was investigated separately. This paper will analyze the effect jointly to generate a more realistic picture. The use case for all investigations is the GPS L1/CA signal

In this work a model of the tracking loops and the spoofing signal will be provided. Based on that, a complete simulation tool has been developed. In the second part the general settings of the simulations will be shown and a metric will be defined to visualize, which signal — authentic or replica — is tracked by the DLL and PLL. This is necessary due to the fact that the receiver loops will not simply track either the authentic or the duplicate signal but a mixture. The next part will show the results of the simulations. Finally, a conclusion and an outlook are given.

SYSTEM MODEL

The GNSS signal s_i of one satellite i is a bit stream d_i – called navigation message – modulated on a spreading code c_i and further modulated on a carrier signal with frequency f_i. The power normalized expression is given by:

$$s_i(t) = d_i(t)c_i(t)\cos(2\pi f_i t) \tag{1}$$

The receiver demodulates the signal by generating and mixing a local replica of the spreading code and the carrier signal with the received signal. Due to the relative movement between the satellite and the receiver, the Doppler effect has to be taken into account and the local replicas need to be continuously readjusted to the received signal.

Tracking loops

A classical GNSS receiver uses two tracking loops to do the synchronization: One to track the carrier signal – usually a PLL and/or an FLL – and another one to track the code signal – usually a DLL. Figure 1 shows the demodulation part of the receiver. Both tracking loops are similar: They use a discriminator to estimate the offset between the replica and the received signals and apply a loop filter to smooth the adjustments. The loop filter can be tuned by changing the order of the filter and the loop bandwidth [11, P. 179 sqq.].

The optimal discriminators – in a maximum likelihood sense – for the PLL and FLL are

$$d_{\text{PLL}} = \arctan(\frac{Q_{\text{P}}}{I_{\text{P}}}) \tag{2}$$

and

$$d_{\text{FLL}} = \frac{\arctan 2(I_{\text{P1}}I_{\text{P2}} + Q_{\text{P1}}Q_{\text{P2}}, I_{\text{P1}}Q_{\text{P2}} - I_{\text{P2}}Q_{\text{P1}})}{t_2 - t_1} \tag{3}$$

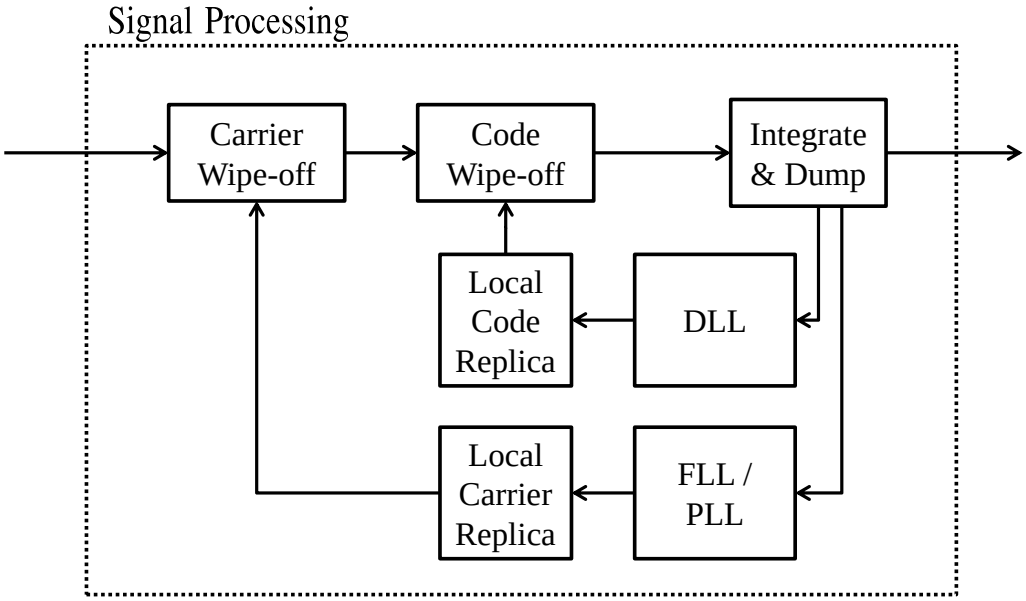


Fig. 1: Signal processing layer of a GNSS receiver.

Q_P describes the real and I_P the imaginary part of the output of the integrate and dump block. In the case of d_FLL two outputs – marked with the subindex 1 and 2 – at subsequent times instances t_1 and t_2 are required.

One common DLL discriminator is the early-minus-late discriminator. To implement it one needs two additional code replicas. One is delayed (late) and the other one is advanced (early) by a defined amount of time. The offset between the early and the late replica is expressed in chips of the PRN code and is referred to as DLL correlator spacing. It can be distinguished between two different types of this discriminator: The non-coherent and the coherent early-minus-late. The later one gives the most accurate code measurement, but can only be used, when the PLL is in phase lock [11, P. 174]. The non-coherent discriminator is given by:

$$d_\mathrm{DLL,NC} = \frac{\sqrt{I_\mathrm{E}^2 + Q_\mathrm{E}^2} - \sqrt{I_\mathrm{L}^2 + Q_\mathrm{L}^2}}{2\sqrt{I_\mathrm{E}^2 + Q_\mathrm{E}^2} + \sqrt{I_\mathrm{L}^2 + Q_\mathrm{L}^2}} \tag{4}$$

The coherent discriminator is given by:

$$d_\mathrm{DLL,C} = \frac{I_\mathrm{E} - I_\mathrm{L}}{4I_\mathrm{P}} \tag{5}$$

Spoofing signal

The spoofing signal has a similar structure like the authentic satellite signal, but is shifted in time by $\Delta\tau_{i,\mathrm{C}}$, has an additional Doppler shift $\Delta f_{i,\mathrm{D}}$ and has a different power level. Normalized to the power of the authentic satellite signal, the spoofing signal can be expressed as:

$$s_{i,\mathrm{spo}}(t) = \sqrt{p_{i,\mathrm{ampl}}} d_i(t + \Delta\tau_{i,\mathrm{C}}) c_i(t + \Delta\tau_{i,\mathrm{C}}) \cos(2\pi(f_i + \Delta f_{i,\mathrm{D}})(t + \Delta\tau_{i,\mathrm{C}})) \tag{6}$$

Where $p_{i,\mathrm{ampl}}$ is the amplification of the spoofer's signal power compared to the authentic signal power.
Due to the similarities the tracking loops can mistake the spoofing signal for an authentic signal and adjust the replicas to track the spoofing signal.

SIMULATIONS AND METHODS

To analyze the behavior of the tracking loops under spoofing, an authentic satellite signal is simulated. After the loop filters of the receiver are in a steady state, a fake satellite signal using the same PRN is added to the authentic signal. Figure 2 shows the generic block diagram of the simulation.

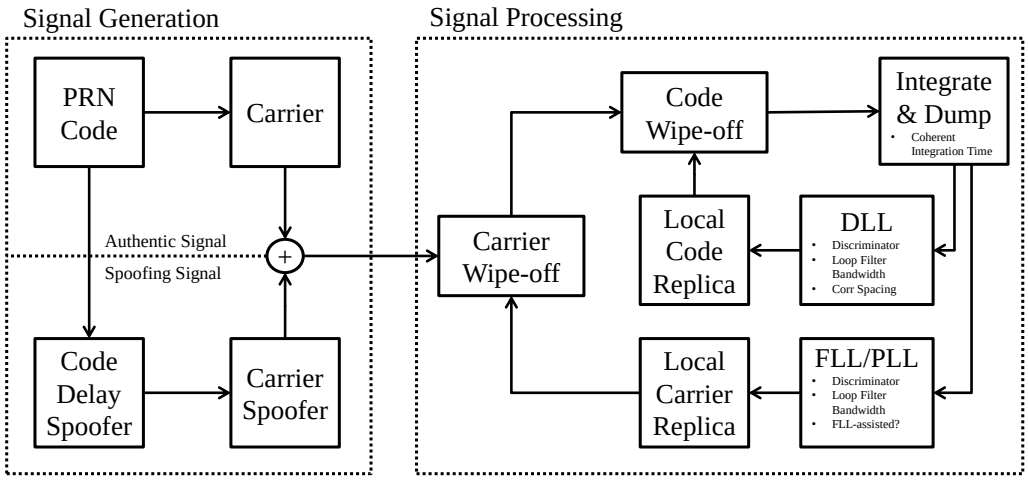


Fig. 2: Flow chart describing the simulation approach.

TABLE I: Settings of the simulated scenarios.

Name	Amplitude [dB]	T_c [ms]	Corr Spacing [chips]	FLL-assisted PLL
Simulation 1	8	5	1	-
Simulation 2	8	5	0.2	-
Simulation 3	8	5	1	x
Simulation 4	8	10	1	-
Simulation 5	3	5	1	-

Main settings

The simulated GPS L1/CA signal is sampled at a rate of $16.368\,\mathrm{MHz}$. It is generated in baseband containing only a Doppler shift. The simulated satellite uses PRN code 1 and is affected by a Doppler frequency of $3500\,\mathrm{Hz}$. The satellite signal is superimposed by Gaussian noise making the simulated satellite signal $27\,\mathrm{dB}$ below the noise floor. After 1 second of simulation time another satellite signal using the same PRN – representing the spoofer – is added. This spoofing signal is affected by an additional Doppler shift of $\Delta f_{i,\mathrm{D}}$ and is delayed by $\Delta\tau_{i,\mathrm{C}}$ compared to the authentic satellite signal. In addition the power of the spoofing signal is variated. These three parameters are the changeable settings of the spoofer. The simulated scenarios are all evaluated for spoofing signals that have an additional Doppler shift $\Delta f_{i,\mathrm{D}}$ between $0\,\mathrm{Hz}$ and $200\,\mathrm{Hz}$ as well as an additional code delay $\Delta\tau_{i,\mathrm{C}}$ between $0\,\mathrm{m}$ and $400\,\mathrm{m}$ compared to the authentic satellite signal. The step sizes for these parameters are $5\,\mathrm{Hz}$ and $10\,\mathrm{m}$. So in total we have 41x41 simulations per scenario.

Scenarios

Table I shows the settings of the simulated scenarios. "Amplitude" stands for the power amplification of the spoofing signal compared to the authentic satellite signal. T_c is the coherent integration time of the signal in the receiver. "Corr Spacing" is the delay between the early and late correlator in chips. The loop filter of the PLL is of third order with a loop bandwidth of $15\,\mathrm{Hz}$ and the loop filter of the DLL is of second order with a bandwidth of $1\,\mathrm{Hz}$. To operate the DLL with a low filter order and bandwidth, so called carrier-aiding is implemented. In case of an involved FLL the PLL changes to an FLL-assisted PLL as described in [11]. The loop filter of the FLL is of second order and has a loop bandwidth of $1\,\mathrm{Hz}$.

There is a pragmatic intention behind the choice of the scenarios: The first scenario describes a basic scenario and in all following scenarios only one parameter – compared to the basic scenario – is changed, so that the changes in the visualization can directly be related to the altered parameter.

Basis for the assessment

Plot 3 shows the behavior of the tracking loops for a code phase delay of $10\,\mathrm{m}$ and an additional Doppler shift of $5\,\mathrm{Hz}$ using the settings of Simulation 1. It can be observed that code and carrier loops switch – after the activation of the spoofing signal – from tracking the authentic signal to tracking the spoofing signal. However, the variance of the replica signal's estimated parameters increases and especially the carrier tracking loop begins to oscillate.

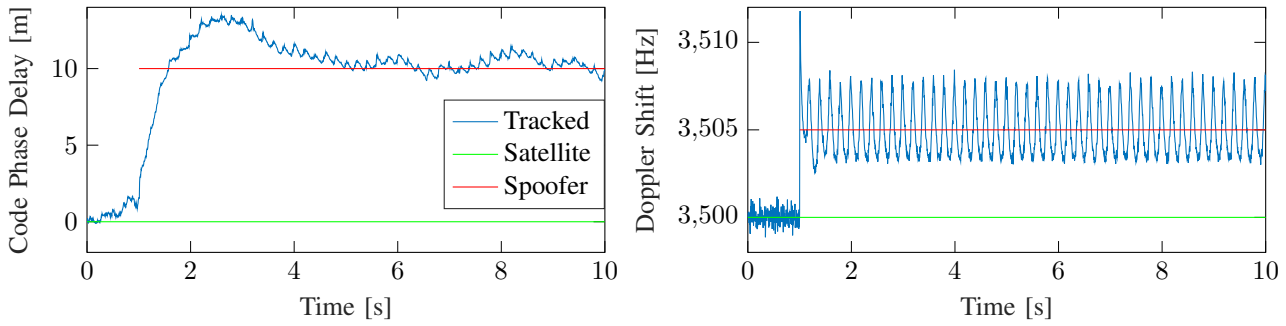


Fig. 3: Simulated code phase delay and carrier Doppler shift of the receiver's replicas for a code phase delay of $10\,\mathrm{m}$ and an additional Doppler shift of $5\,\mathrm{Hz}$ of the spoofing signal using the settings of Simulation 1.

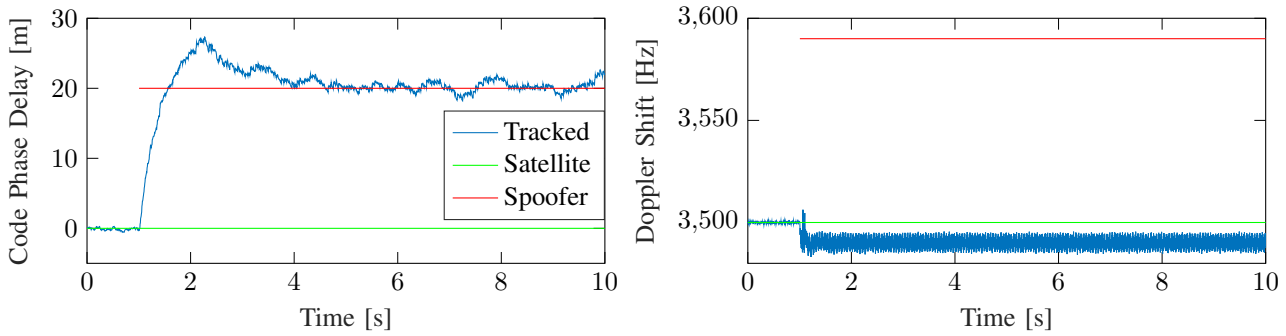


Fig. 4: Simulated code phase delay and carrier Doppler shift of the receiver's replicas for a code phase delay of $20\,\mathrm{m}$ and an additional Doppler shift of $90\,\mathrm{Hz}$ of the spoofing signal using the settings of Simulation 1.

Plot 4 shows the behavior of the tracking loops for a code phase delay of $20\,\mathrm{m}$ and an additional Doppler shift of $90\,\mathrm{Hz}$ using the settings of Simulation 1. Here it can be observed that the code tracking loop switches from the authentic to the spoofing signal, but the carrier tracking loop seems to track a phantom signal slightly below the authentic signal.

In order to visualize the behavior of the tracking loops for a various number of code phase delays and additional Doppler shifts in one plot, the following metrics are defined:

$$m_{\text{Carrier}} = \frac{2f_{\text{NCO}} - (f_{\text{SAT}} + f_{\text{SPO}})}{f_{\text{SPO}} - f_{\text{SAT}}} \tag{7}$$

and

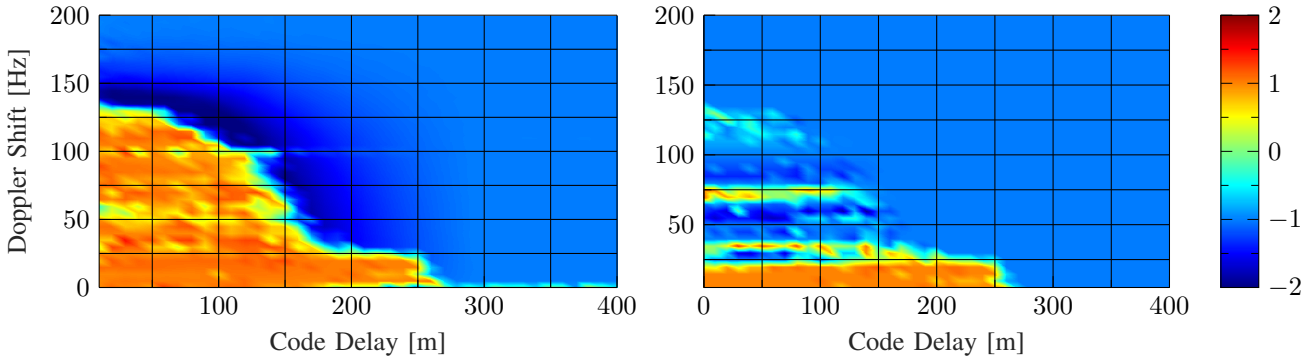
$$m_{\text{Code}} = \frac{2D_{\text{NCO}} - (D_{\text{SAT}} + D_{\text{SPO}})}{D_{\text{SPO}} - D_{\text{SAT}}} \tag{8}$$

f_{NCO}, f_{SAT} and f_{SPO} are the frequencies of the carrier replica in the receiver, of the authentic carrier signal and of the spoofing carrier signal. D_{NCO}, D_{SAT} and D_{SPO} are the phases of the code replica in the receiver, of the authentic code signal and of the spoofing code signal. These six values are averaged over the last second of the simulation.

In cases where the tracking loops lost lock, it can happen that the value of the metric increases extensively. To retain the expressiveness of the visualization, the values of the metric are limited to range of $[-2; +2]$. Values that are outside of the range, are projected to the closest number in the range, i.e. -2 and 2.

The following three values make it easy to understand the metrics:

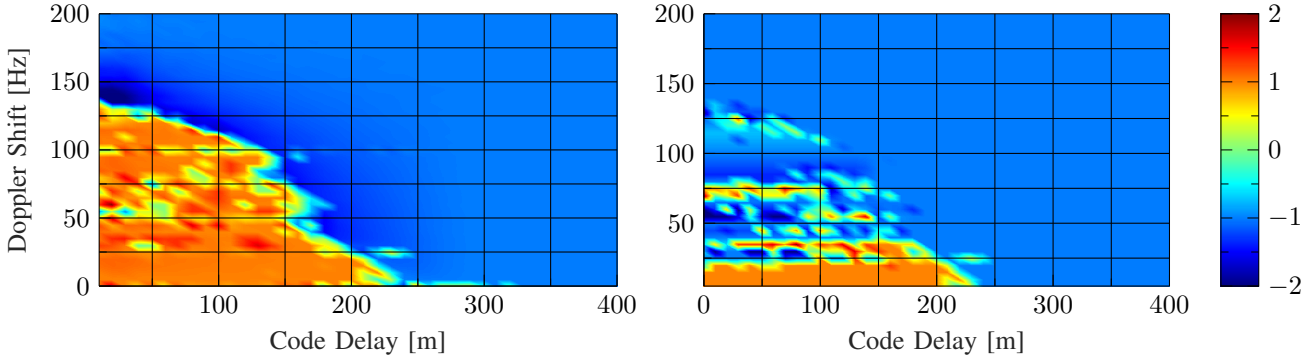
- A value of -1 states that the tracking loop still tracks the authentic signal.
- A value of 1 states that the tracking loop tracks the spoofing signal.
- A value of -2, 0, or 2 states that the behavior of the tracking loop cannot be related to one of the other categories.



(a) Simulation 1: Code Tracking

(b) Simulation 1: Carrier Tracking

Fig. 5: The simulation results using the defined metric for Simulation 1 (reference scenario).



(a) Simulation 2: Code Tracking

(b) Simulation 2: Carrier Tracking

Fig. 6: The simulation results using the defined metric for Simulation 2 (smaller correlator spacing).

SIMULATION RESULTS AND DISCUSSION

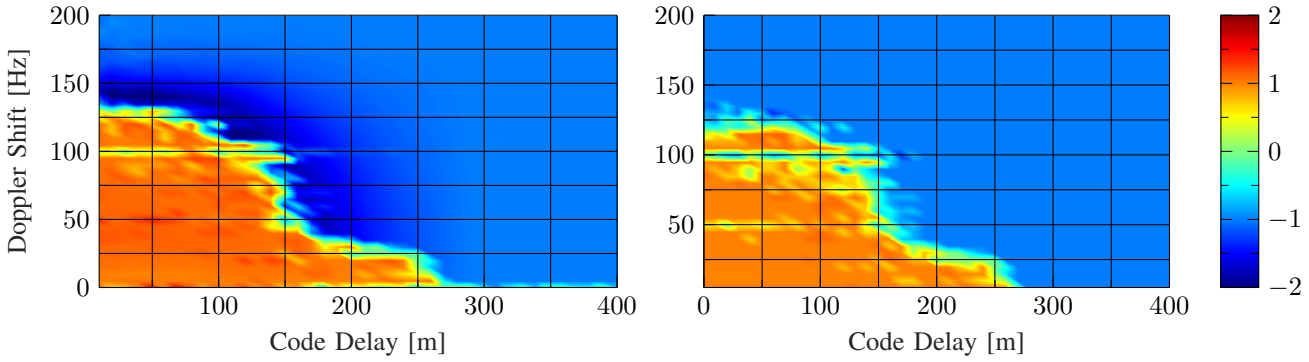
In this section the simulation results using the defined metric are presented and discussed. The simulation results are shown for a selected number of receiver settings corresponding to Table I. On the left hand side the behavior of the code tracking loops and on the right hand side the behavior of the carrier tracking loop is depicted. Relating the plots to the defined metric, a blue color shows the area in which the tracking loop continues to track the authentic signal and an orange color shows the area in which the tracking loop switches to track the spoofing signal.

Simulation 1

Simulation 1 serves as a reference for all further simulations. The corresponding plots are shown in Figure 5. The plot of the code tracking loop shows that an area shaped like a "shoe" in the bottom-left corner of the plot is vulnerable to a spoofing signal: An additional Doppler shift of $0\,\mathrm{Hz}$ to $120\,\mathrm{Hz}$ at low code delays and a code delay of $0\,\mathrm{m}$ to $250\,\mathrm{m}$ at low Doppler shifts. This shape is surrounded by a cyan and dark blue transit area where the code tracking loop neither tracks the authentic nor the spoofing signal.
The plot of the carrier tracking loop identifies a rectangular area in the corner of the plot to be vulnerable to spoofing. The area ranges from $0\,\mathrm{Hz}$ to $20\,\mathrm{Hz}$ in the y-axis and from $0\,\mathrm{m}$ to $250\,\mathrm{m}$ in the x-axis.

Simulation 2

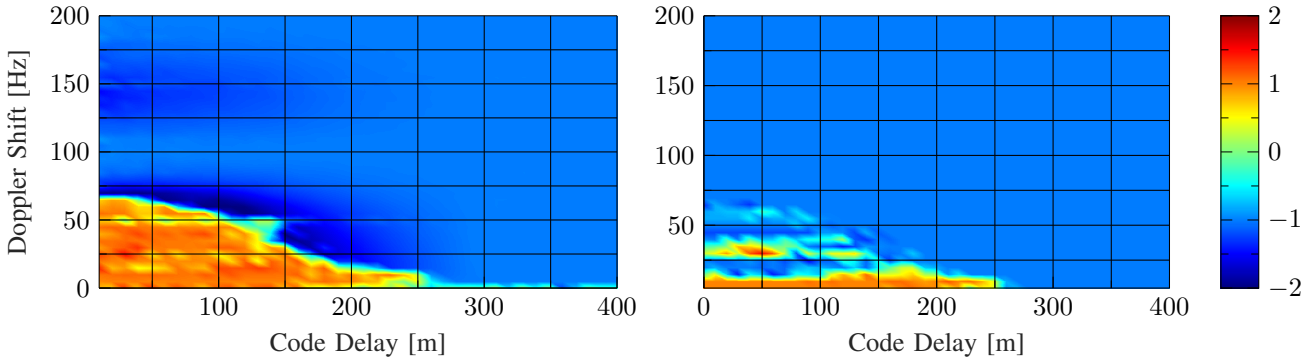
In simulation 2 the correlator spacing between the replica signal early and late has been reduced by a factor of 5 compared to the reference scenario. As can be seen in Figure 6, this change mainly affects the size of the area vulnerable to spoofing in the direction of the x-axis for low Doppler shifts. The upper limit of the range is reduced to $210\,\mathrm{m}$ instead of $250\,\mathrm{m}$.
This effect is quite intuitively: The lower correlator spacing leads to narrower measurement points at the peak of the authentic correlation triangle resulting in smaller impact of the spoofing correlation triangle.



(a) Simulation 3: Code Tracking

(b) Simulation 3: Carrier Tracking

Fig. 7: The simulation results using the defined metric for Simulation 3 (FLL-assisted PLL).



(a) Simulation 4: Code Tracking

(b) Simulation 4: Carrier Tracking

Fig. 8: The simulation results using the defined metric for Simulation 4 (longer T_c).

Simulation 3

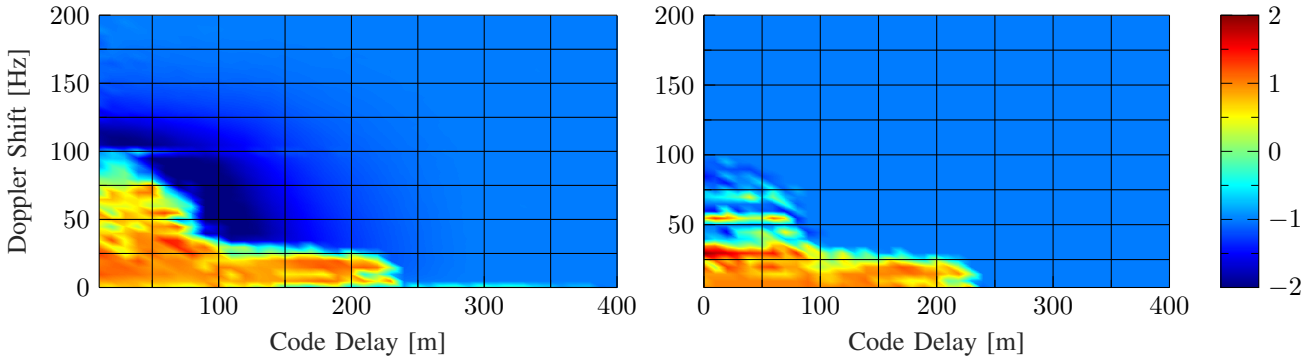
The results for Simulation 3 are shown in Figure 7. The simulated receiver uses an FLL-assisted PLL instead of a pure PLL to track the carrier signal. Therefore, the main difference to the reference scenario is seen in the plot for the carrier tracking: The area, in which the spoofing signal is tracked, is here similar shaped to the one in the code tracking plot. However, it is not surrounded by a dark blue area showing that in the case of the carrier tracking loop the transition from tracking a spoofing to tracking the authentic signal is stricter: Either one of the signals is tracked but not a mixture. This broader area leads to a clearer area of spoofer tracking in the code tracking loop. Clearer means that the area has less yellow blurs corresponding to a firmer tracking of the spoofing signal even with higher additional Doppler frequencies.
This simulated receiver configuration is more robust in dynamic stress conditions but leads to a higher vulnerability to spoofing.

Simulation 4

In simulation 4 the receiver applies a coherent integration time of $10\,\mathrm{ms}$ instead of $5\,\mathrm{ms}$ leading to a more robust tracking of the authentic signal even with a highly synchronous spoofing signal. The corresponding plots are shown in Figure 8. In both plots the area in which the receiver tracks the spoofing signal is halved along the ordinate.
A longer coherent integration time improves the performance of the receiver in low signal-to-noise ratio (SNR) conditions. As shown here, it also complicates a spoofing attack due to the need for a highly synchronous spoofer. However, the coherent integration time cannot be increased limitless due to the bit shifts in the navigation message of the signal and dynamic effects.

Simulation 5

In Simulation 5 the power of the spoofing signal is only twice the power of the authentic signal instead of a factor of 6.3. Figure 9 shows that the area sensitive to tracking the spoofing signal is reduced in comparison to the reference scenario. In the direction of the x-axis it is reduced by $20\,\mathrm{m}$ for small Doppler shifts and even more for higher Doppler shifts. However,



(a) Simulation 5: Code Tracking

(b) Simulation 5: Carrier Tracking

Fig. 9: The simulation results using the defined metric for Simulation 5 (reduced spoofer to authentic signal power ratio).

the transit area – dark blue – in the plot of the code tracking loop is larger.
The signal power of the spoofing signal is not steerable by the receiver. However it is worth noticing that a spoofer with a lower power must be synchronized better with respect to the authentic signal to take over the tracking loops of the receiver. If this degree of synchrony is not achievable, the spoofer will need to increase power revealing it to receivers that are monitoring the SNR.

Summary and Discussion

The investigations show that a small correlator spacing and a long coherent integration time can reduce the vulnerability of a receiver to a spoofing signal – in the matter that the spoofing signal must to be better synchronized to the receiver to take over the tracking loops. An FLL-assisted PLL or any similar approach making the carrier tracking loop more robust against the need of reacquisition will always make it more vulnerable to spoofing as shown in Figure 7. Therefore the simplified answer to the question: "Which GNSS tracking loop configuration is most robust against spoofing?" is: Apply a small correlator spacing and a long coherent integration time and never use an FLL-assisted PLL or any similar approach. However, the detailed answer is not that simple. The parameters cannot be changed arbitrary without losing the ability of the receiver to track the satellite signals at all. The minimum of the correlator spacing is influenced by the bandwidth of received signal: A smaller bandwidth of the received satellite signal reduces the sharpness of the correlation peak [12]. The maximum of the coherent integration time is limited by the user dynamics. Furthermore, in a traditional tracking loop – without using bit prediction – the coherent integration time for the GPS L1/CA signal should not be higher than $20\,\mathrm{ms}$ due to data bit transitions.
In conclusion, one needs to find a tradeoff between the receiver's robustness in highly dynamic stress scenarios and the robustness against a spoofing attack. In addition to a balanced choice of parameters for the receiver, it is always wise to add some algorithms to detect a possible spoofing attack.

CONCLUSION AND OUTLOOK

In this paper a complete simulation tool has been developed to simulate a spoofing attack enabling the test of different receiver settings. The simulations tool includes a metric to visualize the behavior of a receiver's tracking loops in the presence of an authentic and a spoofing signal. Further on, this metric was used to analyze the effect of different receiver settings on the vulnerability of the receiver to a spoofing signal. Finally, a recommendation on the parametrization of the receiver's loops was provided. This answers the question asked in the title: "Which GNSS tracking loop configuration is most robust against spoofing?".

In future research the simulation tool is extended to simulate a more sophisticated tracking architecture. One interesting aspect is to implement a Kalman filter or simply to increase the number of correlators in the code loop architecture from three to five. Furthermore the research can include other signals types with more advanced modulation schemes (i.e. BOC).

ACKNOWLEDGMENT

Parts of the research leading to the results reported in this paper have been elaborated within the project KABUL. We would especially like to thank Mr. Ernst Schmitz on behalf of the German Federal Office of Bundeswehr Equipment, Information Technology and In-Service Support (BAAINBw) for providing the governmental funding. This support is greatly acknowledged.

REFERENCES

[1] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner Jr, "Assessing the spoofing threat: Development of a portable GPS civilian spoofer," in *Proceedings of the ION GNSS International Technical Meeting of the Satellite Division*, vol. 55, 2008, p. 56.

[2] C. Günther, "A Survey of Spoofing and Counter-Measures," *Navigation*, vol. 61, no. 3, pp. 159–177, 2014, ISSN: 2161-4296. DOI: 10.1002/navi.65.

[3] P. J. Teunissen and O. Montenbruck, Eds., *Springer Handbook of Global Navigation Satellite Systems*, Cham: Springer International Publishing, 2017, ISBN: 978-3-319-42926-7 978-3-319-42928-1. DOI: 10.1007/978-3-319-42928-1.

[4] M. L. Psiaki and T. E. Humphreys, "GNSS Spoofing and Detection," *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1258–1270, Jun. 2016, ISSN: 0018-9219. DOI: 10.1109/JPROC.2016.2526658.

[5] M. Meurer, A. Konovaltsev, M. Appel, and M. Cuntz, "Direction-of-Arrival Assisted Sequential Spoofing Detection and Mitigation," p. 12, 2016.

[6] A. Konovaltsev, M. Cuntz, C. Hättich, and M. Meurer, "Autonomous Spoofing Detection and Mitigation in a GNSS Receiver with an Adaptive Antenna Array," presented at the ION GNSS+ 2013, Nashville, TN, USA: The Institute of Navigation, Sep. 30, 2013.

[7] S. Zorn, T. Bamberg, and M. Meurer, "Accurate Position and Attitude Determination in a Jammed or Spoofed Environment Using an Uncalibrated Multi-Antenna-System," *Proceedings of the 2018 International Technical Meeting of The Institute of Navigation*, p. 13, 2018.

[8] M. Cuntz, A. Konovaltsev, and M. Meurer, "Concepts, Development and Validation of Multi-Antenna GNSS Receivers for Resilient Navigation," *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1288–1301, Mar. 24, 2016, ISSN: 0018-9219.

[9] M. Appel, A. Hornbostel, and C. Haettich, "Impact of meaconing and spoofing on Galileo receiver performance," in *7th ESA Workshop on Satellite Navigation Technologies NAVITEC*, 2014.

[10] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "Unmanned Aircraft Capture and Control Via GPS Spoofing," *Journal of Field Robotics*, vol. 31, no. 4, pp. 617–636, Jul. 1, 2014, ISSN: 1556-4967. DOI: 10.1002/rob.21513.

[11] E. Kaplan and C. Hegarty, *Understanding GPS: Principles and Applications*. Artech House, 2005, 718 pp., ISBN: 978-1-58053-895-4.

[12] A. J. V. Dierendonck, P. Fenton, and T. Ford, "Theory and Performance of Narrow Correlator Spacing in a GPS Receiver', Navigation," *Journal of The Institute of Navigation*, 1992.