Received: 8 March 2021 | Revised: 25 October 2021 | Accepted: 12 November 2021

DOI: 10.33012/navi.510

ORIGINAL ARTICLE

Results on GNSS Spoofing Mitigation Using Multiple Receivers

Niklas Stenberg[1] | **Erik Axell**[1] | **Jouni Rantakokko**[1] | **Gustaf Hendeby**[2]

[1] Department of Robust Telecommunications, Swedish Defence Research Agency (FOI), Linköping, Sweden

[2] Department of Electrical Engineering (ISY), Linköping University, Linköping, Sweden

Correspondence
Erik Axell, Swedish Defence Research Agency (FOI), Linköping, Sweden.
Email: erik.axell@foi.se

Summary

GNSS receivers are vulnerable to spoofing attacks in which false satellite signals deceive receivers to compute false position and/or time estimates. This work derives and evaluates algorithms that perform spoofing mitigation by utilizing double differences of pseudorange or carrier phase measurements from multiple receivers. The algorithms identify pseudorange and carrier-phase measurements originating from spoofing signals, and omit these from the position and time computation. The algorithms are evaluated with simulated and live-sky meaconing attacks. The simulated spoofing attacks show that mitigation using pseudoranges is possible in these tests when the receivers are separated by five meters or more. At 20 meters, the pseudorange algorithm correctly authenticates six out of seven pseudoranges within 30 seconds in the same simulator tests. Using carrier phase allows mitigation with shorter distances between receivers, but requires better time synchronization between the receivers. Evaluations with live-sky meaconing attacks show the validity of the proposed mitigation algorithms.

Keywords

carrier phase, double difference, GNSS spoofing, pseudorange, spoofing mitigation

1 | INTRODUCTION

The use of Global Navigation Satellite System (GNSS) receivers has proliferated the last decade and they are used extensively in numerous commercial, as well as safety- and security-related, applications. Spoofing attacks that can deceive GNSS receivers to compute incorrect position and/or time by transmitting false satellite signals constitute a serious threat to modern society (Psiaki & Humphreys, 2016). The possibility of spoofing GNSS receivers using low-cost hardware has been demonstrated by different research groups (see e.g., Humphreys et al. [2008]). GNSS spoofing has, for example, affected many vessels in or close to Russian territorial waters, such as in the Black Sea region (C4ADS, 2019). The emerging threat of GNSS spoofing underlines the importance of developing receivers that are resilient to spoofing attacks.

The work presented herein is focused on spoofing mitigation, however, the mitigation approach is based on well-known spoofing detection algorithms. Several

spoofing detection algorithms that utilize data, such as computed receiver positions (as well as pseudorange or carrier-phase measurements) from multiple receivers have been proposed in the literature, see e.g., Axell et al. (2015a, 2015b), Jahromi et al. (2016), Radin et al. (2015), Swaszek and Hartnett (2013, 2014), Wang et al. (2018), and Wen et al. (2019).

In particular, double differences of pseudoranges or carrier phases are used for spoofing detection in Axell et al. (2015a), Jahromi et al. (2016), Wang et al. (2018), and Wen et al. (2019).

Pseudorange double difference, as well as position solution differences, are used in Axell et al. (2015a) to make a joint decision of whether all receivers are spoofed or not. Spoofing detectors based on double differences of carrier phase and pseudorange as well as power ratio difference are proposed in Wang et al. (2018). Another algorithm for spoofing detection is derived in Wen et al. (2019), also based on pseudorange double differences. The algorithms of Jahromi et al. (2016), Wang et al. (2018), and Wen et al. (2019) use two receivers only. All these works make use of similar signal properties and a *generalized likelihood-ratio test* (GLRT) to make decisions on individual double differences and deal with unknown parameters, and therefore share many common properties.

Moreover, the algorithms of Wang et al. (2018) and Wen et al. (2019) have been used to discriminate individual double differences but do not extend to authenticating individual measurements. Different double-difference tests containing the same pseudorange or phase measurement may result in contradicting decisions and must therefore be combined to make joint decisions on each measurement. Therefore, these algorithms cannot be used without further non-trivial extensions to mitigate attacks like these.

By contrast, the work of Jahromi et al. (2016) makes use of the individual double-difference GLRTs in combination with a graph approach to authenticate individual measurements. However, the graph-based approach assumes that there is only a single measurement for each *pseudorandom noise* (PRN) sequence, which is either spoofed or authentic. Hence, every spoofed PRN can only be detected and possibly excluded from the position, velocity, and time (PVT) computation, but the corresponding authentic measurement for the same PRN cannot be recovered. In Jahromi et al. (2014), carrier-phase double differences were used in a receiver with two antenna elements to mitigate spoofing by first classifying spoofing signals, estimating them, and then subtracting them from the input signal. This requires a two-antenna system and is thus not suitable for a solution with multiple distributed receivers.

When a receiver is subject to a spoofing attack, three scenarios may occur for each PRN sequence (corresponding to a specific satellite); each receiver acquires and tracks: a) the authentic signal only, b) the spoofing signal only, or c) both the authentic and spoofing signals (assuming the receiver has the ability to track multiple correlation peaks). The first case would not pose any problem, since the corresponding satellite signal was not spoofed. In the second case, the authentic signal would not be able to be recovered and included in a PVT solution since it would not be tracked, and the problem would therefore be cast back to a spoofing detection problem. The third case, and the main focus of this paper, poses the problem of deciding which of the received signals would be authentic and which would be spoofed, and to include the authentic signal only in the PVT computation. Detection of authentic and spoofing signals in Case a) and Case b) comes automatically with the spoofing mitigation algorithms proposed in this paper. That is, the proposed algorithms are able to mitigate a spoofing attack in the case of only a single measurement for some PRNs, which is dealt with in Jahromi et al. (2016), but also when two measurements are obtained for all PRNs.

This paper examines spoofing mitigation using pseudorange or carrier-phase measurements from multiple receivers. *Mitigation* refers, in this context, to identifying authentic and spoofing signals, and including authenticated signals only in the resulting PVT solution. In contrast to previous work, it is assumed that the receiver is able to track multiple signals for the same PRN, allowing for reconstruction of the authentic signal while that same PRN sequence is being spoofed. In Ranganathan et al. (2016), spoofing was detected if more than one signal per PRN could be acquired, tracked, and if the separation between the acquired peaks was large enough. That is, the receiver could simultaneously track multiple signals per PRN. Furthermore, this work evaluated spoofing of the GPS L1 C/A signals; however, the algorithm could be readily extended to multi-constellation receivers (e.g., GPS and Galileo) where the double differences could be applied to signals from several constellations. Moreover, in scenarios where only a subset of the GNSS constellations are subjected to a spoofing attack, the pseudorange or carrier-phase measurements for the unspoofed constellations could be authenticated and utilized in the subsequent PVT-calculations.

Modern GNSS receivers already have hundreds of parallel channels to track multiple satellite signals from multiple constellations. Tracking both authentic and spoofing signals requires twice as many tracking channels as a standard receiver. It is therefore a matter of how to make best use of the already available channels or increasing the computational cost by doubling the number of tracking channels. The assumption of tracking both authentic and spoofing signals is necessary for the function of the considered mitigation process. In scenarios where the receiver is not able to track the authentic signal, typically when subjected to high power spoofing signals, the algorithms would still be able to identify the spoofing signals.

The algorithms under consideration in this work were originally derived in our previous papers (Stenberg, 2019) for two receivers and extended in Stenberg et al. (2020) to more than two receivers. These publications developed novel spoofing mitigation algorithms using multiple (≥ 2) GNSS receivers based on previously known spoofing detection algorithms, and evaluated these algorithms in controlled hardware simulations utilizing a Spirent simulator. This paper summarizes and extends the work in Stenberg (2019) and Stenberg et al. (2020) by evaluating the spoofing mitigation approach with live-sky meaconing tests and discussing practical problems and considerations, such as synchronization, for a real-time implementation of the algorithms. Thereby, this paper shows the vailidity of the spoofing mitigation algorithms for practical applications.

The spoofing mitigation algorithms previously developed in Stenberg (2019) and Stenberg et al. (2020) are reiterated in Section 2. The implementation of the algorithms is described in Section 3, and the experimental setup and results are shown in Section 4. The live-sky meaconing test setup and results are described in Section 5, while practical considerations for the algorithms are discussed in Section 6. Section 7 concludes this work.

2 | SYSTEM MODEL AND PROPOSED ALGORITHMS

A binary hypothesis test was first applied to pseudorange and carrier-phase double differences to identify measurements that were generated by spoofing signals. The unknown parameters were dealt with using the GLRT. The binary decisions were then combined to make a final decision whether each (pseudorange or carrier-phase) measurement was spoofed or authentic.

2.1 | Assumptions

The following assumptions are made in this work:

- The spoofing system utilizes a single transmit antenna.
- There are $R \geq 2$ receivers that simultaneously receive authentic and spoofing signals from the same set of PRN sequences (i.e., satellites).
- The receivers are time synchronized or their measurements can be interpolated to common time epochs.
- No multipath errors are present.
- The receivers track both authentic and spoofing signals simultaneously for each satellite.

These assumptions ensure that measurements are available from authentic and spoofing signals for each satellite at all times and that the double differences resulting from two spoofing signals are time-invariant. This approach is applicable to any GNSS signal; however, in this work it is evaluated for the GPS L1 coarse-acquisition (C/A) signal.

The bare presence of multiple signals encoded with the same PRN sequence is enough to declare the occurrence of a spoofing attack. However, to mitigate spoofing (i.e., recover authentic signals while being under attack by a spoofer), a more complex algorithm must be introduced. The proposed algorithm is designed to select the correct signals among the set of both authentic and spoofing signals. That way mitigation is performed by computing the authentic navigation solution based on the identified authentic signals.

2.2 | Models of Authentic and Spoofed GNSS Measurements

The geometric distance between receiver i and satellite k at time n is denoted by $r_i^k[n]$. The range to satellite k, induced by the spoofing signal at the transmitting antenna of the spoofing system, is denoted $\tilde{r}^k[n]$. The distance between receiver i and the spoofing transmission antenna is denoted by $d_i[n]$. Moreover, clock errors in receiver i and satellite k are represented by $t_i[n]$ and $T^k[n]$, respectively. Depending on the type of spoofing attack, different timing errors may occur. For instance, a meaconing system introduces a processing delay while a self-consistent spoofer typically introduces a timing mismatch. The resulting timing error is denoted $T_s[n]$ (where also potential atmospheric effects are included). Ionospheric and tropospheric errors (in meters) are denoted $I_i^k[n]$ and $\zeta_i^k[n]$, respectively, between receiver i and satellite k. The carrier wavelength is denoted by λ.

The pseudorange measurement $\rho_i^k[n]$ in receiver i for satellite signal k is modeled as (adapted from Wang et al. [2018]):

$$\rho_i^k[n] = \tilde{r}^k[n] + d_i[n] + c(t_i[n] - T_s[n]) + \tilde{\epsilon}_i^k[n] \tag{1}$$

when it is generated by a spoofing signal, and:

$$\rho_i^k[n] = r_i^k[n] + c(t_i[n] - T^k[n]) + I_i^k[n] + \zeta_i^k[n] + \epsilon_i^k[n]$$

when it is generated by an authentic signal. The terms $\epsilon_i^k[n]$ and $\tilde{\epsilon}_i^k[n]$ are measurement noise that are assumed to be zero-mean Gaussian noise similarly to Wang et al. (2018). The noise terms are assumed to have approximately the same

variance, thus approximately having the same distribution, and $\epsilon_i^k[n]$ is hereafter used to denote both terms. This is based on the assumption that both the correlation between different PRN sequences and the autocorrelation of the PRN sequences for non-zero delays are negligible.

Let N_i^k and $\tilde{N}_i^k$ denote integers corresponding to the carrier-phase cycle ambiguities between receiver i and satellite k, for authentic and spoofed measurements respectively. The model of the carrier-phase measurement $\phi_i^k[n]$ at time n for receiver i and satellite k is expressed as:

$$\phi_i^k[n] = \tilde{r}^k[n] + d_i[n] + c(t_i[n] - T_s[n]) + \lambda \tilde{N}_i^k + \tilde{\varepsilon}_i^k[n] \tag{2}$$

when the carrier-phase measurement is generated by a spoofing signal (Jahromi et al., 2016), and:

$$\phi_i^k[n] = r_i^k[n] - I_i^k[n] + \zeta_i^k[n] + c(t_i[n] - T^k[n]) + \lambda N_i^k + \varepsilon_i^k[n]$$

when it is generated by an authentic signal. The measurement errors, $\varepsilon_i^k[n]$ and $\tilde{\varepsilon}_i^k[n]$, are assumed to be zero-mean Gaussian noise. The variable $\varepsilon_i^k[n]$ is henceforth used to denote both noise terms, motivated by the PRN correlation properties in analogy with the pseudorange measurements.

2.3 | Identifying Spoofing Signals Based on Double Differences

Double differences of pseudorange or carrier-phase differences are used to identify measurements that have been generated from spoofing signals. The pseudorange single difference between two receivers i and j for satellite k at time n is defined as:

$$\Delta\rho_{ij}^k[n] \triangleq \rho_i^k[n] - \rho_j^k[n]$$

and the double difference for satellite pair k and l is:

$$\nabla\Delta\rho_{ij}^{kl}[n] \triangleq \Delta\rho_{ij}^k[n] - \Delta\rho_{ij}^l[n]$$

This notation is adopted from Jahromi et al. (2016) and Wang et al. (2018). The carrier-phase single and double differences are computed analogously. The individual pseudorange or carrier-phase measurements in the double difference can originate from either authentic or spoofing signals.

Considering two receivers, i and j, and a satellite pair, k and l, the null hypothesis, $\mathcal{H}_0$, is the case where all (pseudorange or carrier-phase) measurements in the double difference are computed from spoofing signals. The alternative hypothesis, $\mathcal{H}_1$, is the case in which at least one measurement in the double difference has been computed from an authentic signal.

2.3.1 | Model of Pseudorange Double Differences

Using the measurement model (1) of the pseudoranges computed from spoofing signals, the double difference under $\mathcal{H}_0$ is:

$$\nabla\Delta\rho_{ij}^{kl}[n] \,\big|\, \mathcal{H}_0 = \nabla\Delta\epsilon_{ij}^{kl}[n]$$

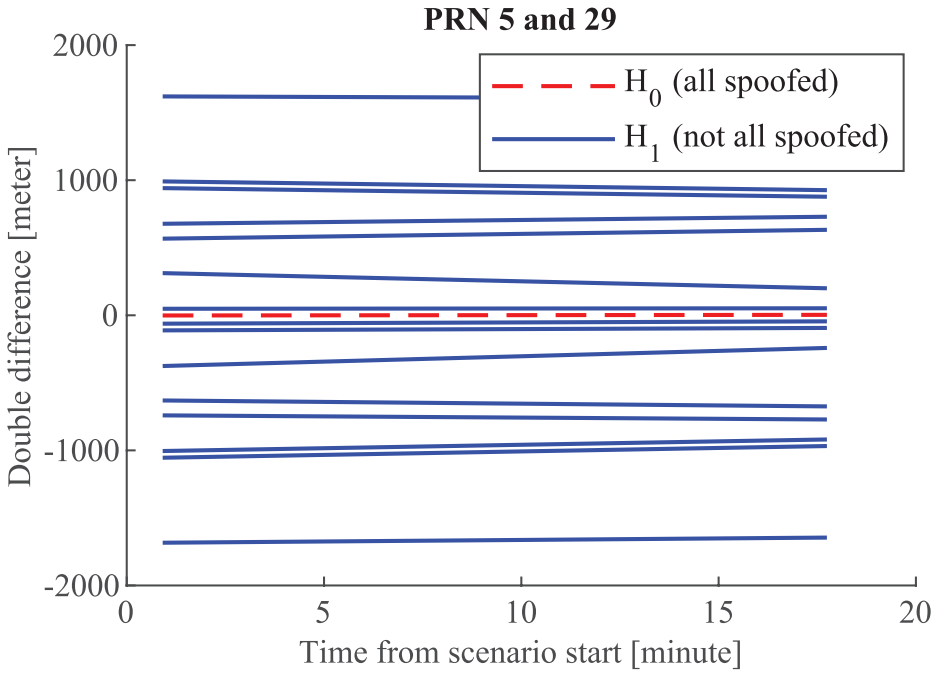

FIGURE 1 Pseudorange double differences in a spoofing scenario for a single satellite pair PRN 5 and 29 and two receivers separated by 100 meters

The double difference $\nabla\Delta\rho_{ij}^{kl}[n]$ under $\mathcal{H}_1$ is generally not zero-mean and does not have a single expression since it encompasses multiple cases. A simple model of it is that it is an affine function in time (for a sufficiently short time duration). This model is motivated by Figure 1 that shows examples of pseudorange double differences. The figure shows pseudorange double differences during a spoofing scenario where both authentic and spoofing signals are tracked. The spoofing system is located 500 m and 600 m, respectively, from the two receivers. The spoofing system also has an additional delay corresponding to 400 m. Double differences of all combinations of authentic and spoofing signals are shown. The double difference under $\mathcal{H}_0$ is close to zero and the differences under $\mathcal{H}_1$ are offset from zero and some of them exhibit slopes.

The pseudorange double differences are therefore modeled as:

$$\nabla\Delta\rho_{ij}^{kl}[n] = \begin{cases} w_\rho[n], & \text{under } \mathcal{H}_0 \\ A_\rho + B_\rho n + w_\rho[n] & \text{under } \mathcal{H}_1 \end{cases} \tag{3}$$

where $n = 1, 2, \ldots, N$ and N defines the length of the observation window; A_ρ and B_ρ are unknown offset and slope coefficients, respectively; and $w_\rho[n] \triangleq \nabla\Delta\epsilon_{ij}^{kl}[n]$. That is, a simple first-order polynomial is used to model the double difference under $\mathcal{H}_1$, which is similar to Wang et al. (2018), who used second-order polynomials for the pseudorange double difference tests. A first-order polynomial is deemed to be a good approximation for the short observation times (in the order of minutes) of practical interest, which is also supported by Figure 1. A_ρ, B_ρ, and w_ρ depend on the receiver pair i and j, and the satellite pair k and l, but this dependence is not explicitly written out in order to simplify the expressions. The noise $w_\rho[n]$ is Gaussian with zero-mean, which follows from the measurement models, and is further assumed to be white.

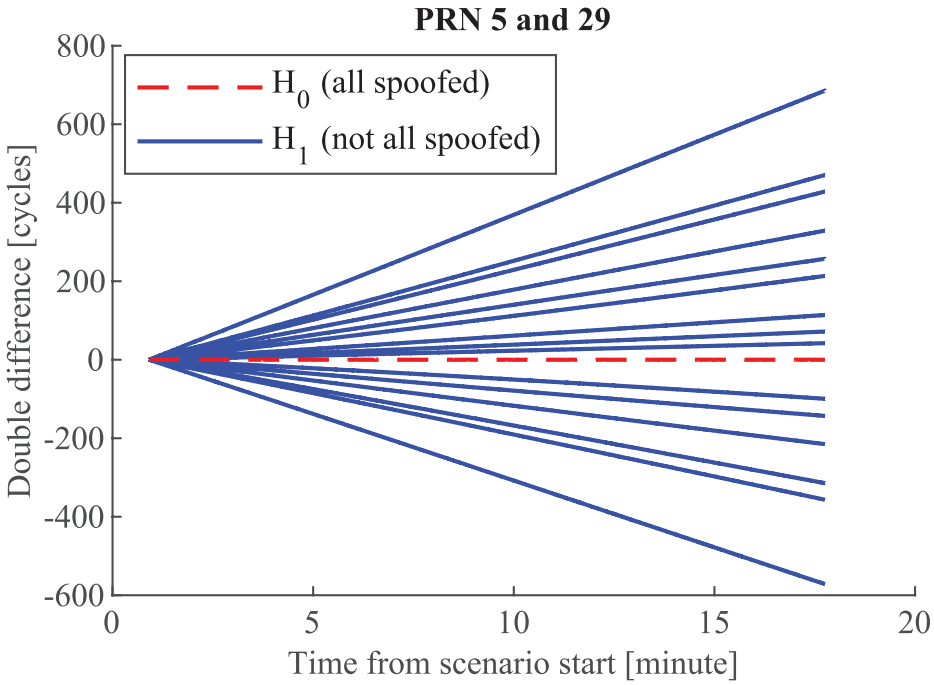

FIGURE 2 Carrier-phase double differences in a spoofing scenario for a single satellite pair PRN 5 and 29 and two receivers separated by 100 meters; each double difference has had its initial value removed to facilitate comparison.

2.3.2 | *Model of Carrier-Phase Double Differences*

The carrier-phase double difference under $\mathcal{H}_0$ is obtained by using the model (2) of carrier phases computed from spoofing signals, and it can be written as:

$$\nabla\Delta\phi_{ij}^{kl}[n]\,\big|\,\mathcal{H}_0 = \lambda\nabla\Delta N_{ij}^{kl} + \nabla\Delta\varepsilon_{ij}^{kl}[n]$$

in which it is assumed that $\lambda\nabla\Delta N_{ij}^{kl}$ is constant during the observation window, as in Jahromi et al. (2016). Examples of carrier-phase double differences are shown in Figure 2, which shows all combinations of double differences for a single spoofing antenna scenario where the receiver tracks both authentic and spoofing signals for all GPS signals. The double difference under $\mathcal{H}_0$ is modeled as a time-invariant offset plus noise, similarly to Jahromi et al. (2016) and further motivated by Figure 2, under $\mathcal{H}_1$, so that:

$$\nabla\Delta\phi_{ij}^{kl}[n] = \begin{cases} A_\phi^0 + w_\phi[n], & \text{under } \mathcal{H}_0 \\ A_\phi^1 + B_\phi^1 n + w_\phi[n] & \text{under } \mathcal{H}_1 \end{cases} \tag{4}$$

where $n = 1, 2, \ldots, N$. A_ϕ^0 and A_ϕ^1 are offsets and B_ϕ^1 is a slope coefficient. The noise $w_\phi[n] \triangleq \nabla\Delta\varepsilon_{ij}^{kl}[n]$ is a zero-mean Gaussian distribution and assumed to be white. $A_\phi^0, A_\phi^1, B_\phi^1$, and w_ϕ depend on the receiver pair *i-j* and the satellite pair *k-l,* but this dependence is not explicitly written out in order to simplify the expressions.

To conclude, the computed double differences, for either pseudorange or carrier-phase measurements, for a certain satellite pair *l-k* and receiver pair *i-j* can be written as:

$$\nabla\Delta(\cdot)_{ij}^{kl}[n] = A_{ij}^{kl} + B_{ij}^{kl} n + w_{ij}^{kl}[n] \tag{5}$$

under both hypotheses. That is, the double differences are modeled as straight lines with slopes B_{ij}^{kl} and offsets A_{ij}^{kl}, for different values of A_{ij}^{kl} and B_{ij}^{kl}.

2.4 | Hypothesis Testing of Double Differences

Without loss of generality, let Receiver 1 be used as a reference, and consider the double differences between all other receivers 2, ... , R for satellites k and l during the complete observation interval $n = 1, ..., N$. These double differences are collected in the matrix:

$$X^{k,l} \triangleq \begin{bmatrix} \nabla\Delta\rho_{21}^{kl}[1] & \nabla\Delta\rho_{31}^{kl}[1] & \dots & \nabla\Delta\rho_{R1}^{kl}[1] \\ \nabla\Delta\rho_{21}^{kl}[2] & \nabla\Delta\rho_{31}^{kl}[2] & \dots & \nabla\Delta\rho_{R1}^{kl}[2] \\ \vdots & \vdots & \ddots & \vdots \\ \nabla\Delta\rho_{21}^{kl}[N] & \nabla\Delta\rho_{31}^{kl}[N] & \dots & \nabla\Delta\rho_{R1}^{kl}[N] \end{bmatrix}$$

The superscripts k and l are omitted in the following for simplicity of notation, so that $X = X^{k,l}$ for a specific (implicit) satellite pair k and l. Also note that the derivation is made for pseudorange measurements, but the model for carrier-phase measurements is equivalent.

The double differences can then be written as:

$$X = \bar{H}\Theta + W \tag{6}$$

with the observation matrix:

$$\bar{H} \triangleq \begin{bmatrix} 1 & 1 & \dots & 1 \\ 1 & 2 & \dots & N \end{bmatrix}^T$$

the parameter matrix:

$$\Theta \triangleq \begin{bmatrix} A_{21}^{kl} & A_{31}^{kl} & \dots & A_{R1}^{kl} \\ B_{21}^{kl} & B_{31}^{kl} & \dots & B_{R1}^{kl} \end{bmatrix}$$

and the noise matrix:

$$W \triangleq \begin{bmatrix} \nabla\Delta\epsilon_{21}^{kl}[1] & \nabla\Delta\epsilon_{31}^{kl}[1] & \cdots & \nabla\Delta\epsilon_{R1}^{kl}[1] \\ \nabla\Delta\epsilon_{21}^{kl}[2] & \nabla\Delta\epsilon_{31}^{kl}[2] & \cdots & \nabla\Delta\epsilon_{R1}^{kl}[2] \\ \vdots & \vdots & \ddots & \vdots \\ \nabla\Delta\epsilon_{21}^{kl}[N] & \nabla\Delta\epsilon_{31}^{kl}[N] & \cdots & \nabla\Delta\epsilon_{R1}^{kl}[N] \end{bmatrix}$$

The measurement model given by Equation (6) is next vectorized as:

$$\begin{aligned} x_{\text{vec}} &\triangleq \text{vec}(X^T) = \text{vec}(\Theta^T \bar{H}^T) + \text{vec}(W^T) \\ &= (\bar{H} \otimes I_{R-1})\text{vec}(\Theta^T) + \text{vec}(W^T) \\ &= H_{\text{vec}}\theta_{\text{vec}} + w_{\text{vec}} \end{aligned} \tag{7}$$

where $H_{\text{vec}} \triangleq (\bar{H} \otimes I_{R-1}), \theta_{\text{vec}} \triangleq \text{vec}(\Theta^T)$ and $w_{\text{vec}} \triangleq \text{vec}(W^T)$. The symbol $\otimes$ denotes the Kronecker product and *vec* denotes vectorization of a matrix by stacking the columns of the matrix in order to form a column vector.

2.4.1 | Pre-Whitening of Linear Batch Model

To be able to apply already derived GLRTs that assume white noise, the linear model is pre-whitened. Let Ω denote the covariance matrix of the noise vector w_{vec}, then:

$$\Omega = \text{cov}(w_{\text{vec}}) = I_N \otimes P$$

assuming that the double differences from different time instances are independent and that the covariance of the noise does not change over the time window that is tested. The matrix P is given by:

$$P = \text{cov}\left(\begin{bmatrix} \nabla\epsilon_2^{kl}[n] - \nabla\epsilon_1^{kl}[n] \\ \nabla\epsilon_3^{kl}[n] - \nabla\epsilon_1^{kl}[n] \\ \vdots \\ \nabla\epsilon_R^{kl}[n] - \nabla\epsilon_1^{kl}[n] \end{bmatrix}\right)$$

where $\nabla\epsilon_i^{kl}[n] = \epsilon_i^k[n] - \epsilon_i^l[n]$. The covariance matrix P can be written:

$$P = \sigma^2 \bar{P}$$

where:

$$\bar{P} \triangleq \begin{bmatrix} 2 & 1 & \cdots & 1 \\ 1 & 2 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 2 \end{bmatrix}$$

assuming that $\text{var}(\nabla\epsilon_i^{kl}[n]) = \sigma^2$ for $i = 1, 2, \ldots, R$ and $\text{cov}(\nabla\epsilon_i^{kl}[n], \nabla\epsilon_j^{kl}[n]) = 0$ for $i \neq j$ and $i, j = 1, 2, \ldots, R$. That is, the noise terms are assumed to be uncorrelated between receivers and as having the same variance in all receivers. The matrix Ω can then be written as:

$$\Omega = I_N \otimes (\sigma^2 \bar{P}) = \sigma^2 (I_N \otimes \bar{P}) = \sigma^2 \bar{\Omega}$$

where $\bar{\Omega} \triangleq (I_N \otimes \bar{P})$. The matrix $\bar{P}$ is positive definite and thus has a square root $\bar{P}^{1/2}$. It is then also possible to write the square root of $\bar{\Omega}$ as:

$$\bar{\Omega}^{1/2} = (I_N \otimes \bar{P})^{1/2} = I_N \otimes \bar{P}^{1/2}$$

It should be noted that any additional information that might be available (e.g., one receiver having larger noise power than the other) can easily be included in the model.

It is possible to pre-whiten Equation (7) using the square root $\bar{\Omega}^{1/2}$, yielding:

$$x = H\theta + w \tag{8}$$

where $x \triangleq \bar{\Omega}^{1/2} x_{\text{vec}}, H \triangleq \bar{\Omega}^{1/2} H_{\text{vec}}$, and $w \triangleq \bar{\Omega}^{1/2} w_{\text{vec}}$ with covariance $\text{cov}(w) = \sigma^2 I$ (Kay, 1998). The final hypothesis test is:

$$\begin{cases} x = H\theta_0 + w & \text{under } \mathcal{H}_0 \\ x = H\theta_1 + w & \text{under } \mathcal{H}_1 \end{cases} \tag{9}$$

where $\theta_0 = 0$ and:

$$\theta_1 = \begin{bmatrix} A_{21}^{kl} & A_{31}^{kl} & \dots & A_{R1}^{kl} & B_{21}^{kl} & B_{31}^{kl} & \dots & B_{R1}^{kl} \end{bmatrix}^T$$

2.4.2 | *Parameter Value Formulation of Hypotheses and Generalized Likelihood Ratio Tests*

Based on the pre-whitened linear batch formulation shown in Equation (8), the hypotheses from Equation (9) can be transformed to hypotheses on the parameter values instead:

$$\begin{cases} C\theta = b & \text{under } \mathcal{H}_0 \\ C\theta \neq b & \text{under } \mathcal{H}_1 \end{cases} \tag{10}$$

where the pseudorange case follows directly as $C = I_{2(R-1)}$ and $b = 0_{2(R-1)\times 1}$. In the carrier-phase case $C = [0_{(R-1)\times(R-1)}\ I_{(R-1)}]$ and $b = 0_{(R-1)\times 1}$ to ignore the effects of the unknown constants present in both hypotheses.

Given the formulation (10) a GLRT can be used to reject $\mathcal{H}_0$ (see Kay [1998] for details). The GLRT was used also in Wang et al. (2018) and Jahromi et al. (2016) for double-difference tests of the pseudorange and carrier-phase measurements, respectively. Assuming that the noise variance σ^2 is known, the GLRT becomes:

$$\frac{(C\hat{\theta} - b)^T [C(H^T H)^{-1} C^T]^{-1} (C\hat{\theta} - b)}{\sigma^2} \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \gamma \tag{11}$$

where $\hat{\theta} = (H^T H)^{-1} H^T x$ is the *maximum likelihood estimate* (MLE) of θ under $\mathcal{H}_1$ (Kay, 1998). The probability of false alarm is in this case given by $P_{\text{FA}} = Q_{\chi_r^2}(\gamma)$ where $Q_{\chi_r^2}$ is the right-tail probability for the χ^2 distribution with r degrees of freedom ($r = 2$ in the pseudorange case and $r = 1$ in the carrier-phase case). The probability of false alarm is the probability of incorrectly rejecting $\mathcal{H}_0$. The threshold in Equation (11) giving the desired probability of false alarm is (Kay, 1998):

$$\gamma = Q_{\chi_r^2}^{-1}(P_{\text{FA}}) \tag{12}$$

If the variance σ^2 is instead considered to be unknown, the GLRT becomes:

$$\frac{N-p}{r} \frac{(C\hat{\theta} - b)^T [C(H^T H)^{-1} C^T]^{-1} (C\hat{\theta} - b)}{x^T (I - H(H^T H)^{-1} H^T) x} \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \gamma \tag{13}$$

where $\hat{\theta} = (H^T H)^{-1} H^T x$ is the MLE of θ under $\mathcal{H}_1$ (Kay, 1998). The probability of false alarm is given by $P_{\text{FA}} = Q_{F_{r,N-p}}(\gamma)$ where $Q_{F_{r,N-p}}$ is the right-tail probability for the F distribution with r numerator and $N-p$ denominator degrees of freedom. Inverting the expression for the probability of false alarm yields a formula for computing the threshold as (Kay, 1998):

$$\gamma = Q_{F_{r,N-p}}^{-1}(P_{\text{FA}}) \tag{14}$$

2.5 | Spoofing Mitigation Based on Double-Difference Hypothesis Tests

The overall spoofing mitigation process, given that there are pseudorange or carrier-phase measurements from both authentic and spoofing signals available, is:

1. For each satellite k, compute all possible pseudorange single differences $\Delta\rho_{ij}^{k}$ or carrier-phase single differences $\Delta\phi_{ij}^{k}$ for the receiver pair i and j. Each satellite gives rise to four single differences for a receiver pair if each receiver tracks two signals per satellite.
2. For each combination of two satellites k and l, compute all possible double differences $\nabla\Delta\rho_{ij}^{kl}$ or $\nabla\Delta\phi_{ij}^{kl}$, respectively. Apply the appropriate GLRT to each double difference. Count the number of times individual pseudorange or carrier-phase measurements belong to double differences where $\mathcal{H}_0$ cannot be rejected.
3. Remove measurements that are counted (indicated to be spoofed) at least $K-1$ times, where K is a predetermined threshold. The criterion is based on the assumption that the spoofing system transmits K or more spoofing satellite signals from a single transmission antenna. In this work, K is set to 4. See below for a further explanation of the parameter K.
4. If more than one (pseudorange or carrier-phase) measurement for a satellite remains at this stage, then the algorithm is unable to identify the authentic signal and the measurements from that satellite should be omitted.
5. All remaining signals are considered authentic (not classified as spoofed), and can be used in the subsequent PVT computations.

A key assumption for the mitigation algorithm and the selection of the threshold K is that the spoofer utilizes a single transmit antenna. That assumption is exploited to identify spoofing signals based on the combination of individual double-difference tests. To mitigate the problem with false identification of spoofing signals, measurements have to be indicated as spoofed $K-1$ times out of all the individual satellite pairs that are tested. If a measurement has been indicated as spoofed $K-1$ times, the test procedure implies that it is originating from the same source as $K-1$ other signals that also have been indicated as spoofing signals. That is, there is a group of K signals originating from the same source.

In the sequel of this work, $K=4$ is chosen based on the assumption that at least four signals are spoofed, which is the minimum number required to compute position and time. A smaller K results in higher risk of signals mistakenly being identified as spoofed, and a larger K results in lower probability of identification of spoofing signals. The principle of requiring measurements to be identified multiple times is similar to the graph approach in Jahromi et al. (2016), where K is the number of vertices (PRNs) connected together due to being identified as spoofing. Different thresholds of the number of connected vertices are investigated in Jahromi et al. (2016), where four is one them.

3 | IMPLEMENTATION

This section briefly describes how the algorithms were implemented and evaluated. For more details on the implementation, see Stenberg (2019). An overview

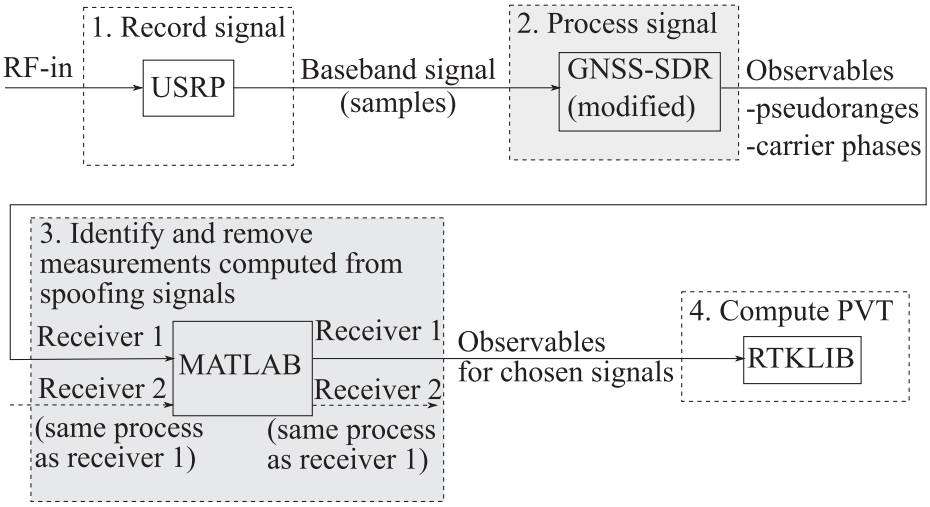

FIGURE 3 Overview of the prototype implementation; this work has made modifications or implementations in the gray blocks whereas the other blocks indicate software or hardware that were used without modifications.

of the prototype implementation is shown in Figure 3. This implementation was used for the simulation tests in Section 4 as well as for the live-sky tests in Section 5.

The open source software-defined GNSS receiver GNSS-SDR[1] was used to compute the pseudorange and carrier-phase measurements. GNSS-SDR (version 0.0.10) was modified to acquire and track both authentic and spoofing signals simultaneously. In Ranganathan et al. (2016), which was mentioned in the introduction, GNSS-SDR was modified and used to acquire and track multiple signals per satellite to perform spoofing detection. The GNSS-SDR project is described in Fernández-Prades et al. (2011). A USRP[2] (universal software radio peripheral) was used as a radio-frequency front-end to record complex baseband samples at 4 MHz that were input to GNSS-SDR.

The proposed mitigation algorithm described in Section 2.5 requires that both the authentic and spoofing signals are tracked in order for the measurements from the spoofing signals to be identified and discarded, ideally leaving only authentic measurements for PVT computation. Computation of the decision statistic can contain measurements from only authentic signals, only spoofing signals, or a combination.

The actual mitigation, consisting of identifying and discarding spoofing measurements, was performed in MATLAB where pseudorange and carrier-phase measurements from GNSS-SDR were taken from GNSS-SDR at a sampling rate of 1 Hz. Measurements from separate receiver runs were synchronized by directly using the time stamps provided by GNSS-SDR for its observed measurements. These time stamps are based on a common reception time across the tracking channels that is set by GNSS-SDR based on a reference satellite[3]. These time stamps were possible to use for evaluation and validation in this test implementation and with the controlled spoofing scenarios that have been evaluated. However, a more robust and accurate time synchronization mechanism is necessary in practice (see Section 6.4 for a discussion about this). Measurements identified as coming from spoofing

[1]See https://gnss-sdr.org/.

[2]https://www.ettus.com/

[3]https://gnss-sdr.org/docs/sp-blocks/observables/

signals were removed in the mitigation process and the remaining measurements were forwarded to the Real-Time Kinematic Library[4] (RTKLIB) for PVT computations. Computations of correct position estimates were verified to work in RTKLIB when the authentic measurements were successfully extracted.

4 | SIMULATION TESTS

This section explains the configurations of the simulated spoofing scenarios as well as the mitigation performance of the proposed algorithms. Seven satellites were tracked in these simulations. Note also that for each of the satellites, two signals were tracked, where seven were authentic signals and seven were spoofing signals.

The four different variations of the proposed GLRT, for pseudorange or carrier-phase measurements and for unknown or known noise variance are evaluated, and denoted Detectors 1a, 1b, 2a, and 2b according to Table 1.

TABLE 1
Different detectors for identification of spoofed measurements

Detector	Measurement	Equation	Noise variance
1a	Pseudorange	(11)	known
1b	Pseudorange	(13)	unknown
2a	Carrier phase	(11)	known
2b	Carrier Phase	(13)	unknown

4.1 | Simulated Scenarios

Simulated meaconing scenarios with different receiver positions were generated with a Spirent GSS9000 GNSS Signal Generator. The Spirent GSS9000 was configured to simultaneously generate both authentic and spoofing signals using its two RF-outputs and functionality of simulating two vehicles. Signals for those satellites seen in the sky by the receiver at the current time and position were simulated.

Scenarios with a stationary receiver and spoofer positions were generated using the parameters given by Table 2. To simulate a processing delay and a delay

TABLE 2
Simulation scenario parameters

Parameter	Value
Start time	01-Jul-2012 20:00:00 UTC
Simulation time	20 min
Base position[a]	59°, 17°, 100 m (lat., lon., height)
Simulated signal	GPS C/A code on the L1 frequency
Satellite orbits	Nominal

[a]The position that the receiver positions are defined in relation to.

[4]http://www.rtklib.com/

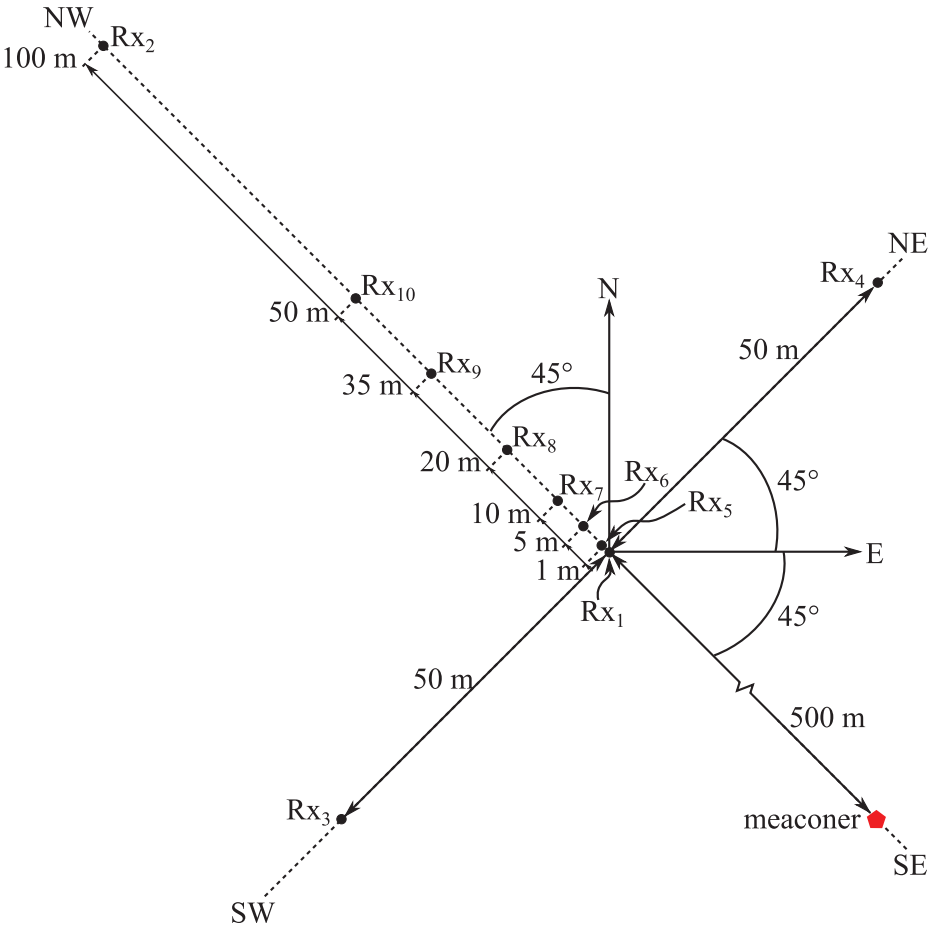

FIGURE 4 Simulated positions of the receivers and the meaconer

between the reception and transmission antennas of the meaconing system, a propagation delay corresponding to 400 meters was added to the spoofing signals in addition to their propagation delay. Noise was not amplified by the simulated spoofing system as it would be in a real meaconing attack, thus the spoofing attacks can also be seen as self-consistent spoofing. In the simulations, no path loss difference for the propagation of the spoofing signals to the different receiver positions were simulated. The difference in distance is small since the receivers are relatively close, so the difference in path loss in an actual setup is insignificant.

The simulated receiver positions (denoted Rx_i) and the position of the meaconer are shown in Figure 4. Each receiver position was simulated once. Different simulations were performed for each receiver and its individual position by essentially running the same scenario but moving the receiver position and adjusting the fixed delay of the spoofing signals accordingly. The simulated receiver positions were combined into different scenarios according to Table 3 to examine the performance in different geometries and with different distances. Both the authentic and the spoofing signals were present from the beginning of the scenarios. The signal power was generated to correspond to the nominal signal power at the surface of the Earth, but with variations depending on satellite elevation. The authentic and spoofing signals were simulated with the same power levels in all scenarios, except in Section 4.2.2, where the impact of differing power levels is evaluated explicitly. Furthermore, realistic live-sky tests are described in Section 5.

TABLE 3
Receivers used in each scenario and the distance between the receivers in each scenario; the direction that the receivers are located on is specified as either SE-NW (southeast to northwest) or SW-NE (southwest to northeast).

Scenario	Receivers	Receiver distance (m)	Direction
1	Rx_1, Rx_2	100	SE-NW
2	Rx_3, Rx_4	100	SW-NE
3	Rx_1, Rx_5	1	SE-NW
4	Rx_1, Rx_6	5	SE-NW
5	Rx_1, Rx_7	10	SE-NW
6	Rx_1, Rx_8	20	SE-NW
7	Rx_1, Rx_9	35	SE-NW
8	Rx_1, Rx_{10}	50	SE-NW

4.2 | Spoofing Mitigation Using Pseudoranges

Initial evaluations were performed to compare Detectors 1a and 1b, assuming known and unknown noise power and using the theoretical thresholds given by Equations (12) and (14), respectively. An average variance from the different scenarios was computed in advance for the double differences under $\mathcal{H}_0$ and used in Detector 1a. The thresholds were set using a probability of false alarm of 1%. Compared to Detector 1b, Detector 1a did not provide consistently better results for all scenarios. Note that the variance of the double differences can vary for different scenarios. Hence, using a test statistic that assumes the variance to be known is usually not well suited in practice. Thus, Detector 1b that assumes the variance to be unknown will be used for the evaluations of the pseudorange algorithm from here on.

4.2.1 | Different Observation Window and Receiver Distances

The average number of correctly authenticated signals (i.e., authentic signals not removed in the mitigation process) using Detector 1b was evaluated for different lengths of observation windows in the different scenarios (see Figure 5). The average number of correctly authenticated signals was used as a performance indicator. It should intuitively improve with increasing observation length, which it does in most cases. The average was calculated over the 20-min simulation duration by dividing it into intervals with the same length as the observation windows under evaluation. That is, less averaging was performed for the evaluations of the longer observation intervals. Since the total number of tracked authentic signals were seven (seven spoofing signals were also tracked), and if, for example, only four authentic signals were correctly authenticated, then three authentic signals would be missed.

Most signals were correctly authenticated within 30 seconds for receivers separated by at least 10 meters. Spoofing signals remaining after the mitigation process were signals that had been incorrectly authenticated. The number of incorrectly authenticated signals was zero for the results in Figure 5 using Detector 1b in all cases, except for receiver distances of 5 meters, using an observation window of 10 seconds, where sporadic erroneous authentications occurred.

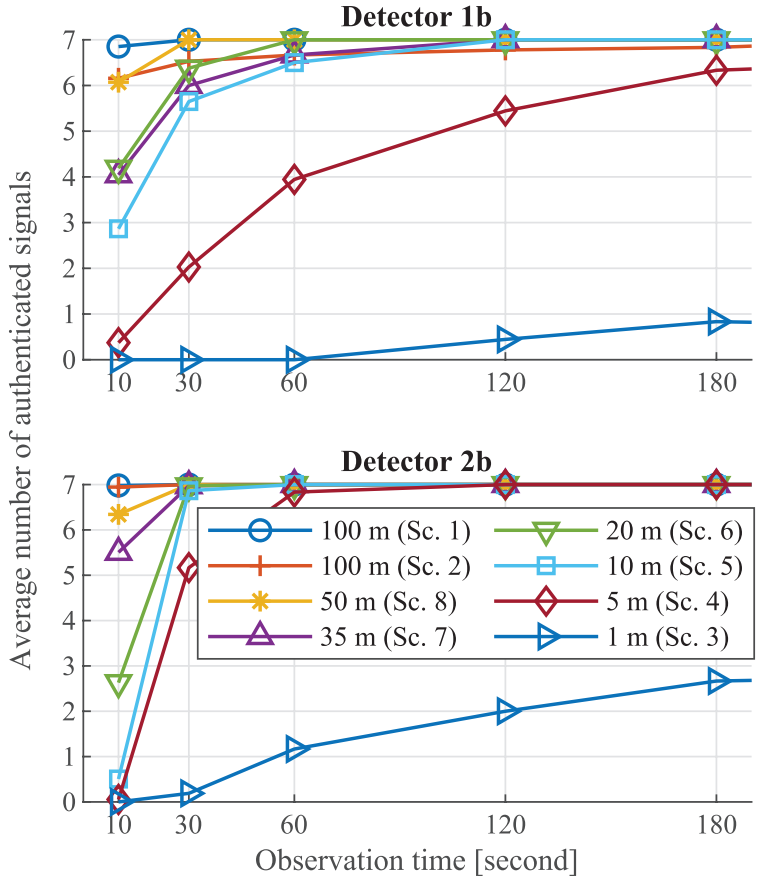

FIGURE 5 The performance of Detector 1b using pseudoranges and Detector 2b using carrier phases for Scenarios (Sc.) 1–8; average number of correctly authenticated signals is shown as a function of the length of the observation window. In total seven authentic and seven spoofing signals were tracked.

The spoofing mitigation approach based on pseudoranges performed well for receiver distances larger than or equal to 5 meters. The slight decrease in performance for the 35-meter distance compared to 20 meters could have been caused by the receiver to satellite geometry in that particular case. More pseudorange double differences under $\mathcal{H}_1$ were close to zero in the former case. The performance in Scenario 1 was better than in Scenario 2, which shows that there is a dependence on the geometry of receivers and spoofing system.

4.2.2 | Spoofing Signals with Different Power Levels

Different power levels of the spoofing signals, −3 dB, +3 dB, +10 dB, and +20 dB relative to the authentic signals, were simulated in separate runs and evaluated for receiver positions Rx_1 and Rx_{10} (separated by 50 meters; Stenberg et al. [2020]). The power level of the spoofing signals was fixed during the simulations. The unmodified version of GNSS-SDR without spoofing mitigation was first evaluated with these simulations. The correct position was computed only in the −3 dB case. It did not compute any position at all in most cases when the spoofing signals and authentic signals had equal power levels, likely because it acquired a mix of authentic and spoofing signals that produced inconsistent sets of measurements. The spoofed position was computed in the +3 dB, +10 dB, and +20 dB cases.

The modified GNSS-SDR was then used to evaluate Detector 1b at different spoofing power levels, using a probability of false alarm set to 0.1%. Observation windows between 30 and 360 seconds were evaluated. The spoofing mitigation algorithm worked well, indicated by the average number of correctly authenticated signals that was close to seven. The performance degraded to in average six correctly authenticated signals only in the +10 dB and +20 dB cases and for the shortest observation interval. The system including the modified GNSS-SDR, as shown in Figure 3, could still calculate the correct position. The number of incorrectly authenticated signals was zero in all cases.

4.3 | Spoofing Mitigation using Carrier Phases

Evaluations of the spoofing mitigation algorithms using the carrier-phase double differences were performed using Detector 2a (assuming known noise variance) and Detector 2b (assuming unknown noise variance). Initial evaluations showed that the theoretical thresholds (using different probabilities of false alarm) did not perform well. The cause was probably that the carrier-phase double differences under $\mathcal{H}_0$ were not perfectly constant during the observation window, as assumed in the hypothesis test. That was likely caused by receiver time synchronization errors between the different receiver runs. The problem of using the theoretical threshold could also be the result of using a linear model for the change over time of double differences and the Gaussian noise assumption, which are simplifications. The results in Wang et al. (2018) also indicated that a more accurate time synchronization is needed for spoofing detection using double differences of carrier phase compared to pseudorange measurements. A more thorough analysis is needed in future work to exactly quantify how the synchronization accuracy and approximation errors of the simplifications affect the theoretical decision threshold and, consequently, the mitigation performance.

However, the distribution of the test statistics under $\mathcal{H}_0$ and $\mathcal{H}_1$ was separate enough to enable separation by setting the threshold empirically. Therefore, the threshold was instead set based on the simulation data to yield a false alarm rate of 1%. That is, the test statistics featured in Equations (11) and (13) were computed based on the available simulation data under $\mathcal{H}_0$. The decision thresholds were then set, based on these computed test statistics, such that the desired false alarm probability was achieved with equality. A single threshold was determined and used for Detector 2a, while it was set individually for each observation length for Detector 2b, in analogy with (12) and (14), considering all scenarios. Detector 2b showed a more consistent performance than Detector 2a and was able to authenticate the signals faster. Furthermore, the performance of Detector 2a decreased for observation windows longer than four minutes in most scenarios. Therefore, results for Detector 2a are not shown in Figure 5, in which the average number of correctly authenticated signals is shown for different observation windows using Detector 2b. The number of incorrectly authenticated signals was zero in all cases for the results in Figure 5 using Detector 2b.

Similarly to the pseudorange evaluations, longer observation windows and receiver distances provide better performance in most cases. The performance decreases for some of the longer observation windows, which could be caused by the small time variations of double differences under $\mathcal{H}_0$, which are more noticeable for longer observation times. The model of the double difference as affine in time under $\mathcal{H}_1$ is less accurate over long time windows, which also affects the performance negatively.

4.4 | Spoofing Mitigation with Two and More Receivers

The performance can be improved by using more than two receivers. The mitigation approach was evaluated next using more than two receivers, using Detector 1b (i.e., pseudorange measurements and assuming the noise variance is unknown). The theoretical thresholds were used with $P_{FA} = 1\%$. The combinations of receivers that had a minimum separation of 5- and 50-meter distances according to Table 4 were evaluated (see Figure 6). The number of incorrectly authenticated signals in the 5-meter scenario was zero for observation times of 30 seconds and longer, but occurred sporadically for the shorter observation times. No signals were incorrectly authenticated in the 50-meter scenario. As seen in Figure 6, increasing the number of receivers significantly improves the performance for closely spaced receivers. For widely spaced receivers, the addition of extra receivers has the potential to improve the number of authenticated signals for short observation windows.

TABLE 4
Combination of multiple receivers; the reference receiver is underlined. Distance equates to distance to reference receiver.

Distance	Receivers	Combinations
5	1,6,7	{1, 6}, {6, 7}, {1, 6, 7}
50	1,3,4,10	{1, 4}, {1, 10}, {1, 4, 10}, ... {1, 3, 4, 10}

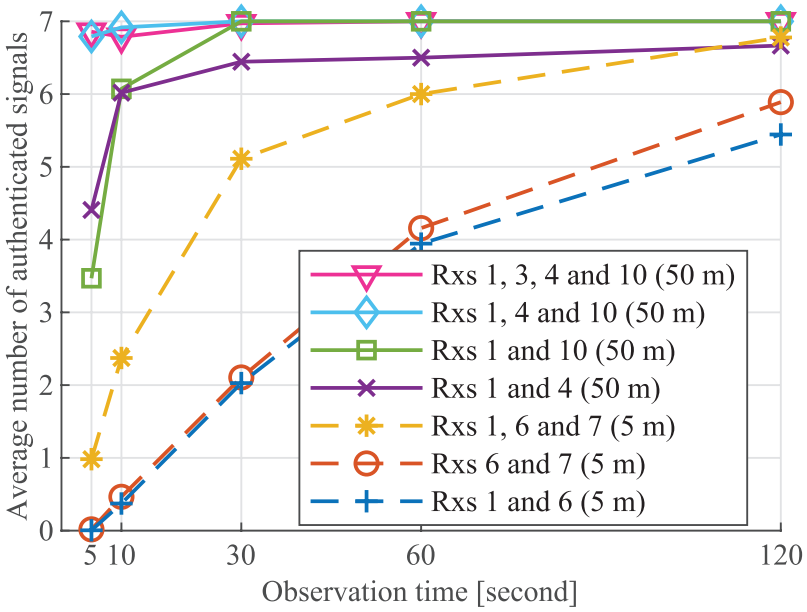

FIGURE 6 Average number of correctly authenticated signals as a function of observation time; the scenario with receivers 1, 6, and 7 (5-meter distances) used Receiver 6 as reference. The scenario with receivers 1, 3, 4, and 10 (50-meter distances) used Receiver 1 as reference. In total, seven authentic and seven spoofing signals were tracked.

5 | LIVE-SKY TESTS

In addition to the simulated spoofing attacks, evaluations have also been done with live-sky signals and spoofing attacks performed as real over-the-air meaconing (replay) attacks. The tests were performed at Vidsel Test Range in Sweden during the fall of 2019.

5.1 | Live-Sky Meaconing Scenarios

The spoofing tests were performed as replay-attacks where the spoofed position was about 900 m from the authentic positions. The spoofing system introduced delays to the spoofing signals equivalent of approximately one kilometer between the spoofer and the receivers under attack. Since the spoofing tests were performed as replay-attacks, the spoofing signals were those signals received by the spoofing system's receiver antenna. Since the spoofing system was close to the victim receivers, the spoofing signals matched more or less the same authentic satellite signals as seen by the victim receivers.

Complex baseband samples were recorded using USRP B210 with a sample rate of 4 MHz at the L1 frequency simultaneously for different static antenna positions. Two receiver pairs were considered in the evaluations. The first pair consisted of receivers denoted *Rx A* and *Rx B,* separated by approximately 50 m. The second receiver pair evaluated consisted of receivers *Rx A* and *Rx C,* separated by approximately 15 m. The receiver positions, as well as the position of the receiver and transmitting antennas of the spoofing system, are shown in Figure 7. Evaluations were performed using pseudorange measurements, and assuming the noise variance to be unknown (i.e., Detector 1b).

The spoofing power was ramped (2 dB every 30 seconds) during the test. The rather short time duration on each power level resulted in a time window in which two correlation peaks (authentic and spoofed) were visible simultaneously for quite a short time. In total, 40 power levels were used on both the up and down intervals, and the max power was maintained for five minutes.

The mitigation worked only on the intervals of the meaconing tests in which the correlation peaks from both the authentic and spoofing signals could be acquired simultaneously (i.e., when the spoofing power was not too high or too

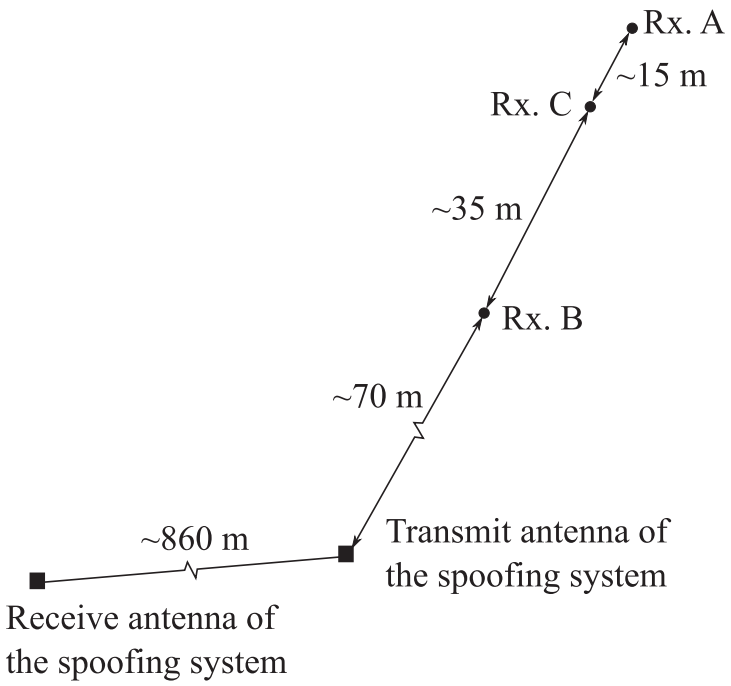

FIGURE 7 Receiver positions and the position of transmitting and receiver antennas of spoofing system in live-sky tests

low). Therefore, evaluations were performed on subintervals of the meaconing tests. In that respect, the algorithm is more suited for spoofing in which the spoofing power is not much higher than the authentic signals. In these cases, longer authentication windows might be possible, and hence it is more likely that two correlation peaks would be visible simultaneously in two (or more) receivers for multiple satellites.

5.2 | Estimated Jammer-to-Noise Power Ratio

The *jammer-to-noise power ratio,* denoted J/N, was estimated in the tests to gain an idea of how the power ramp was experienced at the receivers. It should be noted that the more general and commonly used terms *jammer-to-noise* and *J/N* are used to denote the power ratio, although the attack consists of spoofing only. The J/N was estimated based on the baseband I/Q samples recorded by the USRPs. The received power, denoted P_r, was estimated and averaged over the 30-s ramp steps. The noise power, denoted by P_n, was estimated as the average of P_r in an interval before the meaconing started. J/N in dB was estimated as $10\log_{10}((P_r - P_n)/P_n)$.

See Figure 8 for an example of the estimated J/N. Note the nonlinearities in the beginning and end of the ramp and that the USRP became saturated for high spoofing powers. The steps in the estimated J/N were close to the expected 2 dB in the middle of the ramp up and down parts. The shown theoretical ramp was adjusted to match these steps that were close to 2 dB.

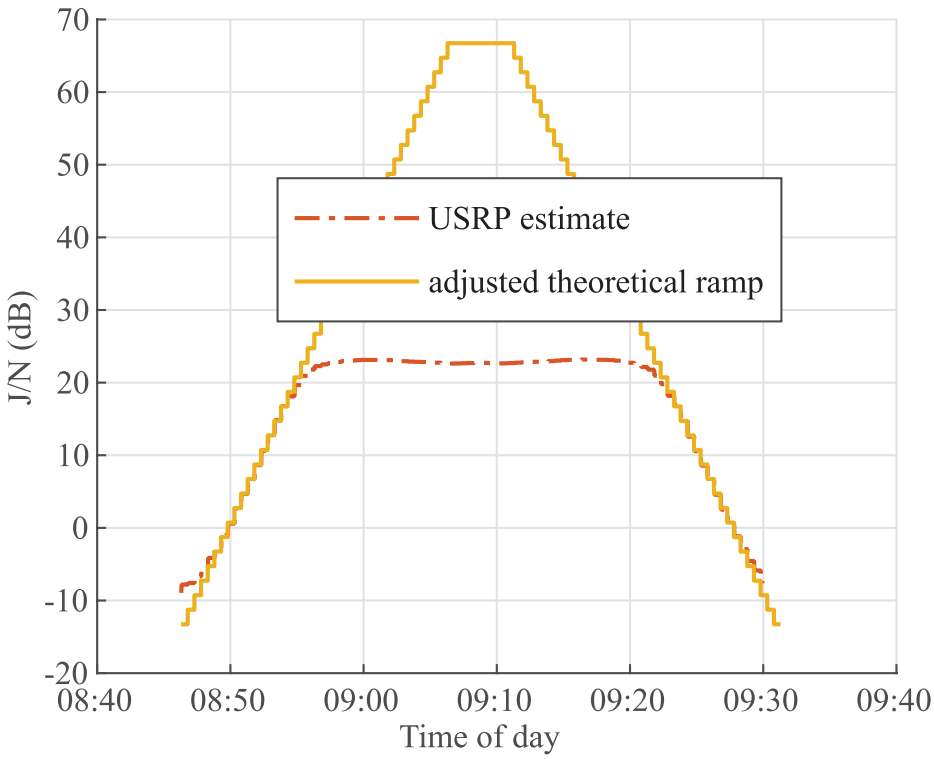

FIGURE 8 Estimated J/N using receiver Rx B over 30-s ramp steps showing a theoretical ramp adjusted with the help of the USRP-estimated J/N

5.3 | Results with Unmodified Receivers in the Meaconing Tests

In a scenario in which the spoofing power is ramped up and then down, a (normal) receiver (e.g., unmodified GNSS-SDR) initially locks onto the authentic satellite signals when there are no spoofing signals present, and provides PVT solutions consistent with the true state of the receiver. When the power transmitted from the spoofing system is increased and becomes high enough, the receiver eventually locks onto the spoofing signals and start computing an incorrect (spoofed) position. Next, the power transmitted from the spoofing system is ramped down and the receiver eventually loses lock of the spoofing signals (not necessarily at the same time). The receiver can then lock onto the authentic signals and true PVT solutions are eventually computed.

Results for the unmodified version of GNSS-SDR are shown in Figure 9. The figure shows the estimated J/N and the horizontal position error. The computed positions did not switch back to the true position in this particular test due to the tracking loops still being locked on to the spoofing signals that were still strong enough to be tracked, but the receiver was just about to lose the spoofing position as seen by the increasing variations of the position error at the end of the test.

There are (small) intervals in which both authentic and spoofing signals have approximately the same power during the ramp-up and ramp-down phases. It is possible to acquire spoofing signals as well as the authentic signals in these intervals and use them to evaluate the algorithm. Figure 10 shows an example of the (acquisition) correlation function of a one-time instance during such an interval for receiver Rx A. The figure shows two visible correlation peaks corresponding to the authentic and spoofing signal, respectively.

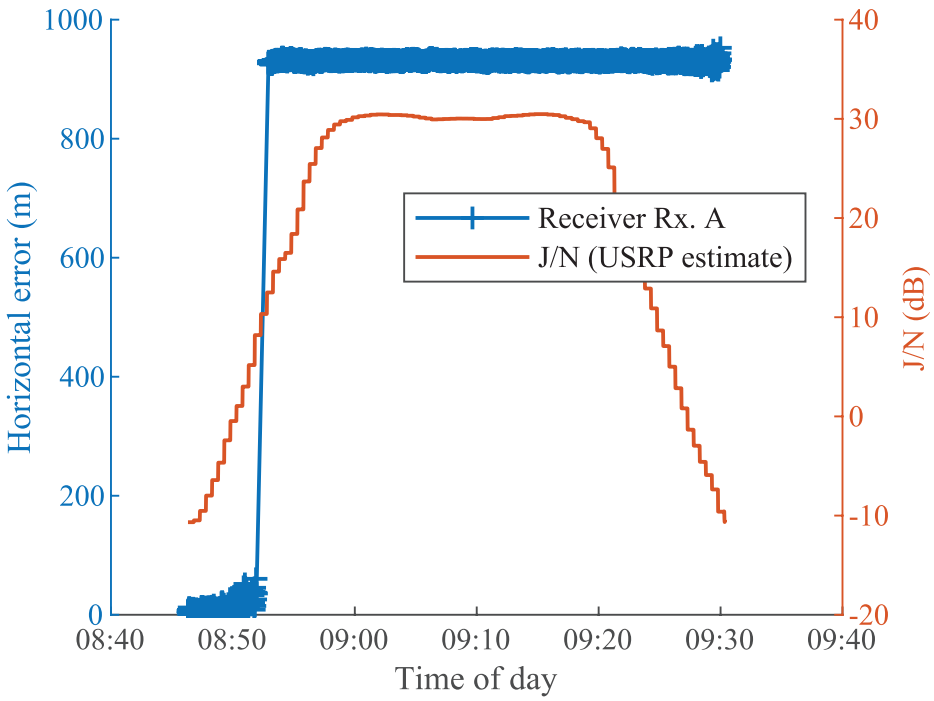

FIGURE 9 Horizontal position error based on position computations from GNSS-SDR; ramp in J/N (dB) based on USRP data with averaging over the 30-s ramp steps

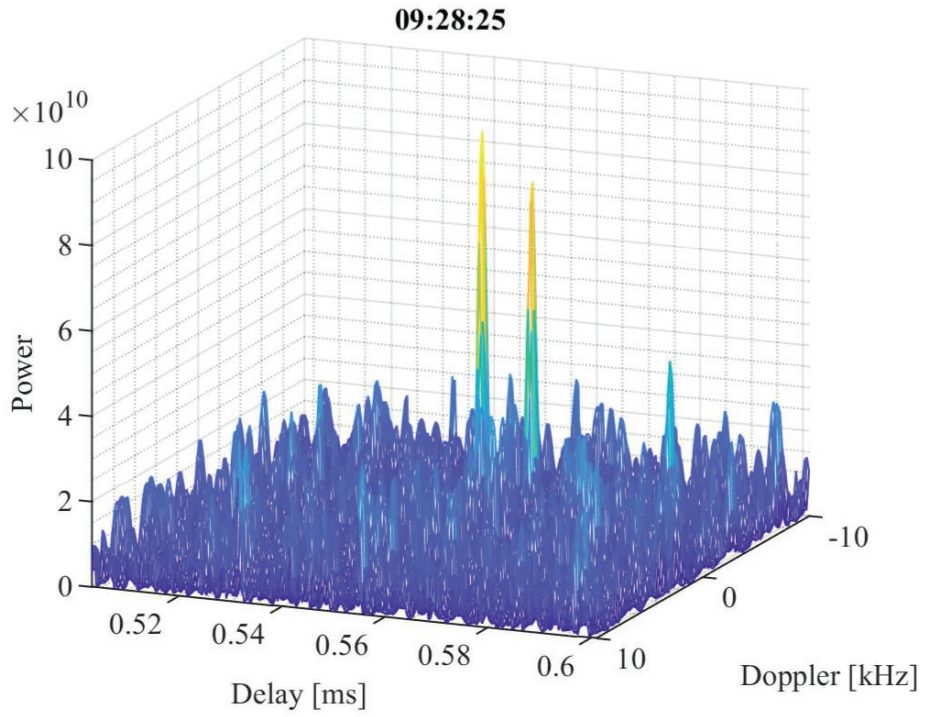

FIGURE 10 Correlation function at time instance 09:28:25, receiver Rx A and PRN 1

5.4 | Evaluation of Spoofing Mitigation on the Ramp-Down Part of the Meaconing Tests

Consider the end of a test in which the spoofing power is ramped down. Only spoofing signals are possible to acquire initially, but the authentic signals eventually become available when the spoofing power is decreased. However, the receiver might still track the spoofing signals and provide incorrect PVT solutions. The modified version of GNSS-SDR, with the proposed spoofing mitigation algorithms, can be run to acquire and track weaker authentic signals. When the modified GNSS-SDR has acquired two signals per satellite for multiple satellites during the ramp-down process, the mitigation algorithms identify the spoofing signals and discard them, leaving authentic signals for the computation of position estimates.

The most notable improvement of using the mitigation algorithm is achieved on the ramp-down portion of these tests. The unmodified version of GNSS-SDR kept tracking authentic signals on the ramp-up part until the authentic signals became essentially unusable. Therefore, there was no clear improvement in the ability to continue computing true position estimates on the ramp-up part using the mitigation process compared to using the unmodified version of GNSS-SDR.

The first receiver pair with receivers Rx A and Rx B were used to evaluate the end of the ramp test. The receivers were separated by approximately 50 m. Receiver Rx B was placed approximately 70 m from the spoofing transmit antenna and Rx A approximately 70 + 50 m from the spoofing transmit antenna. The algorithm was run on a 15-second observation interval based on authentication of five satellites that were tracked by both receivers.

Horizontal error after spoofing mitigation using RTKLIB as well as using the unmodified GNSS-SDR is shown in Figures 11 and 12. Note that less frequent position solutions are produced in the unmodified GNSS-SDR which uses the spoofing signals when their power decreases. The J/N is also shown, estimated using the

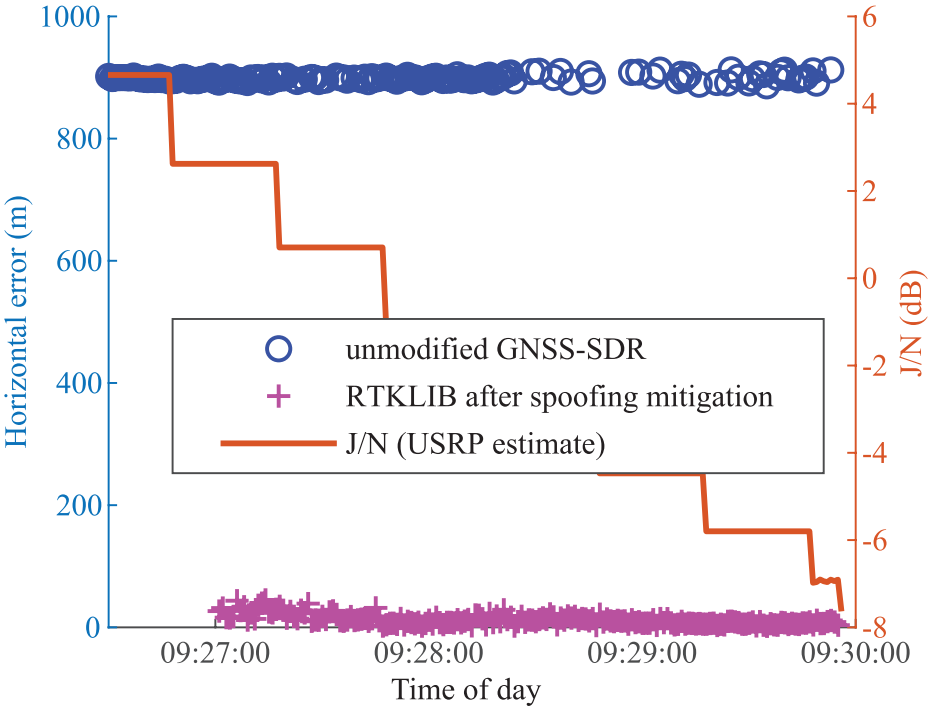

FIGURE 11 Horizontal error with receiver Rx B and estimated J/N using averaging over the 30-s ramp intervals

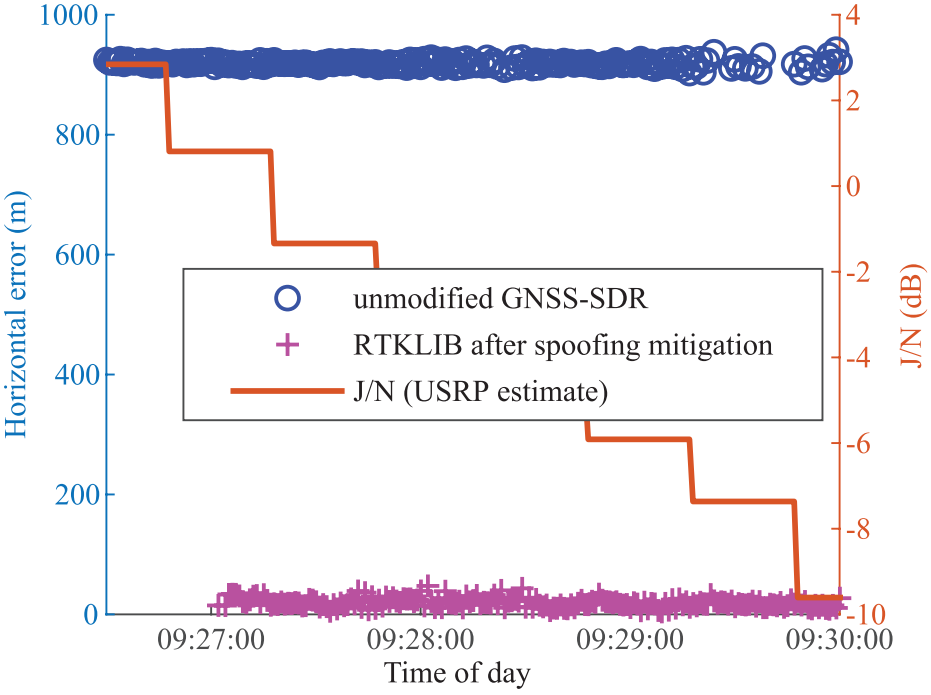

FIGURE 12 Horizontal error with receiver Rx A and estimated J/N using averaging over the 30-s ramp intervals

USRPI/Q data with averaging over the 30-second ramp intervals. Mitigated position solutions are available from about 09:27:00 at 2.7 dB J/N for receiver Rx B and 0.8 dB for receiver Rx A (different USRPs and different locations). Note that the different evaluated power levels in Section 4.2.2 were stated per satellite as the ratio

of spoofing power to authentic signal power and that the two highest are comparable to the levels achieved here. The observation window used for mitigation is included in the time period of the mitigated position solutions shown (mitigation observation windows starts at about 09:27:00).

In these evaluations, five satellites were used. Both the authentic satellite signal and the spoofing signal was present for all five satellites in both receivers over the analyzed time interval. The algorithm makes mitigated position solutions available over an additional J/N range spanning several dB, in which the unmodified receiver does not compute correct position estimates. Similar results were obtained with receivers separated by approximately 12 meters (both approximately 85 meters away from the spoofing systems' antenna) in another similar ramp test.

The earliest time that the mitigated true position can be computed is determined by how many mitigated satellite signals are necessary to compute the PVT (which would generally require at least four). If only four would have been required, the mitigation processes could run slightly earlier (maybe 30 seconds), but would yield worse position accuracy. The time for first mitigated position solution is determined by when (pseudorange) measurements from the authentic, initially weaker, signals begin being possible to acquire.

5.5 | Using the Algorithm for Spoofing Detection

Mitigation using the proposed algorithm is not possible when the spoofing power is too high since the authentic signals cannot be acquired and tracked. However, the algorithm can detect the spoofing attack. Running the algorithm with only one signal per satellite performs spoofing detection. Spoofing is detected if the algorithm removes more than a certain number of signals. The satellite signals can be considered authenticated if they are not removed.

Consider the second receiver pair, consisting of receivers Rx A and Rx C, from the evaluated ramp test, that were separated by about 15 m. In the middle of this scenario, when both receivers are locked onto the spoofing signals and are computing the spoofed position, the algorithm can be used to detect spoofing. Considering eight common satellites between the two receivers during the middle of the ramp (a 27-minute interval), the algorithm detects all of these satellites as spoofed based on 30-second observation intervals.

6 | PRACTICAL CONSIDERATIONS AND IMPLEMENTATION ASPECTS

For an actual real-time implementation of the proposed mitigation algorithms, there are some practical aspects that need to be dealt with. These aspects are discussed in the following, together with some requirements and propositions for how they can be solved by slight modifications to the algorithms using additional logic.

6.1 | The Receivers do not Track the Same Set of Satellites or the Same Satellite Signals

The mitigation approach requires two signals, an authentic and a spoofing signal, for each satellite and receiver that can be used to generate pseudorange or carrier-phase measurements. This is necessary for all satellites that are needed to

compute a PVT solution. Signals from the same satellites have to be tracked in all cooperating receivers.

A problem that may occur due to different signal blockage conditions is that one particular satellite signal might not be visible by all receivers at the same time. Furthermore, both the authentic and spoofing signals for a particular satellite might not be visible at one receiver, let alone at multiple receivers simultaneously. Only an authentic or a spoofing signal might be visible to some receivers. These situations can occur in urban environments or hilly terrain, especially with widely spaced receivers. To handle these kind of problems, more logic to combine signals from different satellites that are visible in different time intervals is needed.

When more than two receivers are used, satellites can be combined in different ways, and the proposed algorithms should be modified to comply with this. For example, two receivers running the mitigation algorithm can only authenticate satellites that are tracked by both receivers. If the two receivers track two different sets of satellites S_1 and S_2, then the algorithm can be run initially on the intersection of these two sets. Then, a third receiver could be used to authenticate the remaining satellites in S_1 or S_2 if the third receiver tracks some of these satellites.

To be able to identify a spoofing signal using the double differences, both receivers have to track the spoofing signal in the case of two receivers cooperating. This can also pose a problem if more than two receivers are tested simultaneously and all but one receiver track the spoofing signal for a particular satellite. Including the receiver that does not track the spoofing signal in the mitigation process would decrease the chance of the spoofing signal being identified. Thus, if it is likely that receivers are tracking different sets of signals, it might be better to perform pairwise testing of receivers. Further analysis of how to combine different sets of receivers and signals in different types of scenarios is required in future work.

Note also that it is straightforward to extend the algorithm to allow the use of multiple spoofing signals per satellite, although at the cost of an increased computational complexity.

6.2 | Spoofing Signals Remaining After the Mitigation Process

If a spoofing signal remains after running the spoofing mitigation algorithm (not identified by spoofing algorithm), it could possibly be removed by a simple receiver autonomous integrity monitoring (RAIM) check since its pseudorange will not be consistent with other pseudoranges belonging to the authentic signals.

An extra level of protection could be obtained by running other spoofing detection algorithms (Psiaki & Humphreys, 2016), exploiting other principles or some similar algorithm using pseudoranges or PVT solutions with multiple receivers to detect spoofing on the measurements chosen by the spoofing mitigation algorithm to detect if spoofing signals remain among the authenticated measurements.

6.3 | Multipath Effects and Overlapping Correlation Peaks

Multipath effects are not considered in the mitigation algorithm. Multipath could cause extra separate correlation peaks that could be acquired and tracked as additional signals for some satellites. These extra signals would not be mitigated by the proposed algorithm and would have to be removed or discarded by some other method. Multipath effects could also distort the correlation peaks corresponding to

the authentic signal for small multipath delays. This could lead to a degradation of accuracy for the pseudorange and carrier-phase measurements.

Some types of spoofing attacks and scenarios may also cause overlapping correlation peaks that cannot be separated by the receiver. This could, for instance, occur during an intermediate attack with a portable receiver-spoofer where the correlation peak of the spoofing signal initially is aligned with the one corresponding to the authentic signal (Humphreys et al., 2008). The performance of the mitigation algorithm in the previous described scenarios with overlapping correlation peaks needs to be examined further.

6.4 | Time Synchronization

The proposed spoofing mitigation algorithm relies on the exchange of measurements between cooperating time synchronized receivers. In Wang et al. (2018), it was shown that the pseudorange approach required time synchronization between the receivers on the order of one millisecond. In comparison, a synchronization error below one microsecond is desired when using carrier-phase measurements.

Modern mass-market receivers, which utilize multiple constellations and frequencies (such as the u-blox F9), are able to provide a timing accuracy of 5–10 ns during favorable conditions. Furthermore, if the receivers are subjected to spoofing signals, they are still able to deliver a sufficiently accurate PVT solution as long as the spoofing mitigation algorithm can successfully track both authentic and spoofing signals and choose the authentic signals for subsequent processing. However, when experiencing a high-power jamming or spoofing signal, the receivers would not be able to provide a PVT solution. Due to the low-quality temperature controlled crystal oscillators (TCXO) utilized in the majority of receivers, they would experience a rapidly increasing timing error during outages. TCXO with one ppm accuracy are typically used in GNSS receivers which translates to an error of 3–4 ms per hour. Hence, an improved timing holdover capability is desired. Note that after a GNSS outage has occurred, it is recommended that the pseudorange approach be employed at least initially since the timing requirements become less stringent.

The examined algorithm can be utilized in two set-ups, either one in which multiple receivers are integrated on a single vehicle (or on a stationary site) or one in which multiple vehicles are equipped with a single receiver. In the former case, wired solutions could be utilized for exchanging measurements, which would also enable multiple options for solving time synchronization. In the latter case, the available solutions would depend heavily on the application and scenario at hand but a multitude of options would be available. One possibility would be to integrate a higher-quality (GNSS-disciplined) oscillator to provide the required holdover functionality. High-quality oven-controlled crystal oscillators (OCXO), which are used in time servers, can exhibit a holdover time accuracy down to 5 μs after 24 hours (European GNSS Agency, 2020). Furthermore, chip scale atomic clocks (CSACs) are being integrated in some safety and security applications.

CSACs such as the Microsemi SA.45s are small, lightweight, and energy efficient compared to rubidium atomic clocks, but they exhibit similar performance as shown in Littleton-Strand et al. (2021). Atomic clocks can provide one μs accuracy for almost 24 hours (European GNSS Agency, 2020). Hence, from a technology standpoint, it is possible to obtain a sufficient time synchronization for the spoofing mitigation algorithm. However, the time accuracy becomes a trade-off between the quality and cost of the oscillator, but it should be feasible to provide an accuracy

better than 1 ms for a few hours at a reasonable complexity and cost by utilizing a high-quality TCXO or a low-end OCXO.

Another option would be to perform time synchronization in a distributed manner using wireless communication links (European GNSS Agency, 2020). Ultra-wideband (UWB) transceivers, such as Decawave's DW1000 that adheres to the IEEE 802.15.4a standard, provide a low-cost alternative for exchanging data and performing accurate time synchronization in line-of-sight conditions at short ranges (up to a few hundred meters). In order to provide decimeter-level ranging accuracies, UWB transceivers synchronize themselves internally with an accuracy of a few ns (see e.g., Zhao et al. [2020]). In Bonafini et al. (2018), it was shown that time synchronization with a maximum jitter of 3.3 μs and a standard deviation of 0.7 μs was obtainable by using standard UWB transceivers amongst all nodes in the network. Hence, a swarm of small unmanned aerial vehicles (UAVs) that predominantly operates in line-of-sight conditions can utilize low-cost, lightweight UWB-transceivers for data exchange and synchronization.

Also, the 3GPP standard specifies the possibility for network providers to provide 10 μs time synchronization accuracy in the *Fine Time Assistance* mode as a part of the network-assisted GNSS service, which could eventually be utilized if similar spoofing mitigation technologies are implemented in smartphone GNSS receivers (ETSI, 2019).

6.5 | Stationary vs. Mobile Applications

The current implementation requires both authentic and spoofing signals to be tracked simultaneously for a number of satellites during an observation window. This is harder to guarantee for mobile receivers than for stationary receivers, for example in urban scenarios where the spoofing signals or the authentic signals might be blocked intermittently. However, the algorithm is applicable to some mobile scenarios (e.g., for ships moving in open environments). To handle more general scenarios, extra logic would have to be implemented to allow for signals to be intermittently blocked from view.

6.6 | When to Run the Mitigation Algorithm?

The algorithm can be run continuously, periodically, or whenever it is deemed necessary based on certain triggering events (e.g., loss of lock or after spoofing has been detected). The computational resources that are available should be considered. Continuous authentication could be used to obtain extra robustness against false signals and to fuse authentication results over time to obtain more accurate results. It is expected that the algorithm could be run in real time. The computational complexity is quadratic in the number of signals that should be authenticated in the case of two receivers.

7 | CONCLUSION

GNSS spoofing mitigation algorithms using either pseudorange or carrier-phase double differences from multiple receivers have been derived, evaluated, and shown to perform well in the evaluated scenarios. The proposed mitigation algorithms identify pseudorange and carrier-phase measurements originating from

spoofing signals, and suppress the attack by omitting these from the PVT computation. Identification of spoofed measurements is based on a combination of individual double-difference tests of multiple receivers and satellites. Simulated spoofing attacks show that accurate mitigation is possible using pseudoranges and at least five meters between the receivers.

Simulation results show that the mitigation performance is improved when the distance between the receivers, alternatively if the observation interval, increases. Moreover, the results showed that improvements in mitigation performance is possible also by increasing the number of receivers exchanging information, especially for closely spaced receivers or short observation intervals. Furthermore, spoofing mitigation using carrier-phase double differences can allow for mitigation with distances shorter than five meters between the receivers, but this approach requires a higher synchronization accuracy between the receivers. Mitigation should be theoretically possible at decimeter-level distances with the use of carrier-phase double differences and good enough synchronization accuracy, since the carrier wavelength of the GPS L1 C/A signal is about 2 dm.

Evaluations were done not only by simulation, but also conducted using live-sky meaconing attacks that confirmed the validity of the mitigation process. The algorithm was shown to be able to identify and remove measurements caused by spoofing signals and thereafter compute position estimates consistent with the true position. Furthermore, the mitigation algorithm allowed for recovery of the true position at higher spoofing signal powers compared to GNSS-SDR running without the mitigation algorithm.

REFERENCES

Axell, E., Alexandersson, M., & Lindgren, T. (2015a). Results on GNSS meaconing detection with multiple COTS receivers. *2015 International Conference on Localization and GNSS (ICL-GNSS)*, Gothenburg, Sweden. https://www.doi.org/10.1109/ICL-GNSS.2015.7217162

Axell, E., Larsson, E. G., & Persson, D. (2015b). GNSS spoofing detection using multiple mobile COTS receivers. *2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP),* South Brisbane, QLD. https://www.doi.org/10.1109/ICASSP.2015.7178560

Bonafini, F., Ferrari, P., Flammini, A., Rinaldi, S., & Sisinni, E. (2018). Exploiting time synchronization as side effect in UWB real-time localization devices. *2018 IEEE International Symposium on Precision Clock Synchronization for Measurement, Control, and Communication (ISPCS),* Geneva, Switzerland. https://www.doi.org/10.1109/ISPCS.2018.8543074

C4ADS. (2019). *Above us only stars: Exposing GPS spoofing in Russia and Syria.* C4ADS. https://www.c4reports.org/aboveusonlystars

European GNSS Agency. (2020). *GNSS user technology report: Editor's special on space data for Europe, 3.* https://www.euspa.europa.eu/sites/default/files/uploads/technology_report_2020.pdf

European Technical Standard (ETSI). (2019). *Requirements for support of assisted global navigation satellite system* (Technical Standard No. 138171-V15.1.0). https://www.mystandards.biz/standard/etsits-138171-v15-1-0-7.5.2019.html

Fernández-Prades, C., Arribas, J., Closas, P., Avilés, C., & Esteve, L. (2011). GNSS-SDR: An open source tool for researchers and developers. *Proc. of the 24th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2011),* Portland, OR, 780–794. https://www.ion.org/publications/abstract.cfm?articleID=9640

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),* Savannah, GA, 2314–2325. https://www.ion.org/publications/abstract.cfm?articleID=8132

Jahromi, A. J., Broumandan, A., Daneshmand, S., Sokhandan, N., & Lachapelle, G. (2014). A double antenna approach toward detection, classification, and mitigation of GNSS structural interference. *Proc. of the 6th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC)*, Noordwijk, The Netherlands. https://schulich.ucalgary.ca/labs/position-location-and-navigation/files/position-location-and-navigation/jafarnia2014_conference.pdf

Jahromi, A. J., Broumandan, A., & Lachapelle, G. (2016). GNSS signal authenticity verification using carrier phase measurements with multiple receivers. *8th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC),* Noordwijk, The Netherlands. https://www.doi.org/10.1109/NAVITEC.2016.7849323

Kay, S. M. (1998). *Fundamentals of Statistical Signal Processing, Volume II: Detection Theory*. Pearson.

Littleton-Strand, L., Nedelkov, F., Griggs, E., & Akos, D. (2021). Exploring the chip scale atomic clock within a GPS disciplined oscillator. *Proc. of the 2021 International Technical Meeting of The Institute of Navigation,* 254–268. https://www.doi.org/10.33012/2021.17831

Psiaki, M. L., & Humphreys, T. E. (2016). GNSS spoofing and detection. *Proc. of the IEEE, 104*(6), 1258–1270. https://www.doi.org/10.1109/JPROC.2016.2526658

Radin, D., Swaszek, P. F., Seals, K. C., & Hartnett, R. J. (2015). GNSS spoof detection based on pseudoranges from multiple receivers. *Proc. of the 2015 International Technical Meeting of the Institute of Navigation,* Dana Point, CA, 657–671. https://www.ion.org/publications/abstract.cfm?articleID=12658

Ranganathan, A., Ólafsdóttir, H., & Capkun, S. (2016). SPREE: a spoofing resistant GPS receiver. *Proc. of the 22nd Annual International Conference on Mobile Computing and Networking,* 348–360. https://doi.org/10.1145/2973750.2973753

Stenberg, N. (2019). *Spoofing mitigation using multiple GNSS-receivers* [Master's thesis, Linköping University]. https://liu.diva-portal.org/smash/get/diva2:1333664/FULLTEXT01.pdf

Stenberg, N., Axell, E., Rantakokko, J., & Hendeby, G. (2020). GNSS spoofing mitigation using multiple receivers. *2020 IEEE/ION Position, Location and Navigation Symposium (PLANS)*, Portland, OR. https://www.doi.org/10.1109/PLANS46316.2020.9109958

Swaszek, P. F., & Hartnett, R. J. (2013). Spoof detection using multiple COTS receivers in safety critical applications. *Proc. of the 26th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+)*, Nashville, TN, 2921–2930. https://www.ion.org/publications/abstract.cfm?articleID=11221

Swaszek, P. F., & Hartnett, R. J. (2014). A multiple COTS receiver GNSS spoof detector – Extensions. *Proc. of the 2014 International Technical Meeting of the Institute of Navigation*, San Diego, CA, 316–326. https://www.ion.org/publications/abstract.cfm?articleID=11501

Wang, F., Li, H., & Lu, M. (2018). GNSS spoofing detection based on unsynchronized double-antenna measurements. *IEEE Access, 6,* 31203–31212. https://www.doi.org/10.1109/ACCESS.2018.2845365

Wen, J., Li, H., Wang, Z., & Lu, M. (2019). Spoofing discrimination using multiple independent receivers based on code-based pseudorange measurements. *Proc. of the 32nd International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+),* Miami, FL, 3892–3903. https://www.doi.org/10.33012/2019.17075

Zhao, K., Zhao, T., Zheng, Z., Yu, C., Ma, D., Rabie, K., & Kharel, R. (2020). Optimization of time synchronization and algorithms with TDOA based indoor positioning technique for internet of things. *Sensors, 20*(22). https://www.doi.org/10.3390/s20226513

How to cite this article: Stenberg, N., Axell, E., Rantakokko, J., & Hendeby, G. (2022) Results on GNSS spoofing mitigation using multiple receivers. *NAVIGATION, 69*(1). https://doi.org/10.33012/navi.510