GNSS Spoofing Mitigation Using Multiple Receivers

Niklas Stenberg, Erik Axell, Jouni Rantakokko and Gustaf Hendeby

Stenberg, N., Axell, E., Rantakokko, J., Hendeby, G., (2020), GNSS Spoofing Mitigation Using Multiple Receivers, *Proceedings of 2020 IEEE/ION Position, Location and Navigation Symposium (PLANS)*, , 555-565. https://doi.org/10.1109/PLANS46316.2020.9109958

Original publication available at:
https://doi.org/10.1109/PLANS46316.2020.9109958

GNSS Spoofing Mitigation Using Multiple Receivers

Niklas Stenberg*, Erik Axell*, Jouni Rantakokko* and Gustaf Hendeby†
*Dept. of Robust Telecommunications,
Swedish Defence Research Agency (FOI), Linköping, Sweden
{niklas.stenberg, erik.axell, jouni.rantakokko}@foi.se
†Dept. of Electrical Engineering (ISY),
Linköping University, Linköping, Sweden
gustaf.hendeby@liu.se

***Abstract*—GNSS receivers are vulnerable to spoofing attacks, where false satellite signals are transmitted to trick the receiver to provide false position and/or time estimates. Novel algorithms are proposed for spoofing mitigation by exchanging double differences of pseudorange, or carrier phase, measurements between multiple GNSS receivers. In scenarios where the spoofing system utilizes a single transmit antenna, the pseudorange, and carrier phase, measurements that are associated with the spoofing signal can be detected and removed. Simulated meaconing attacks generated with a Spirent hardware simulator and measurements obtained with a modified version of GNSS-SDR are used to evaluate the proposed algorithms. Spoofing mitigation using pseudorange measurements is possible, for receivers that are separated at least five meters apart. With a receiver separation of 20 meters, the pseudorange double difference algorithm is able to correctly authenticate at least six of seven pseudoranges within 30 seconds. The carrier phase approach enables mitigation of spoofing signals at shorter receiver distances. However, this approach requires a more accurate time synchronization between the receivers.**

***Index Terms*—GNSS spoofing, spoofing mitigation, pseudorange, carrier phase, double differences**

I. Introduction

Global Navigation Satellite System (GNSS) receivers are currently used in a vast number of civilian, safety and security related applications. GNSS receivers are vulnerable to spoofing attacks where false satellite signals are transmitted and the receiver can be tricked to provide false position and/or time estimates [1]. Several research groups have demonstrated the ability to spoof GNSS receivers with low-cost hardware, see e.g. [2]. Furthermore, a large number of vessels have been affected by spoofing attacks when traveling in or near Russian territorial waters, e.g. in the Black Sea [3]. Spoofing attacks could have serious implications, both in navigation and timing applications; hence, it is important to develop GNSS receivers that are robust against spoofing attacks.

There are different types of spoofing, e.g. self-consistent (simulator) spoofing and meaconing. A self-consistent spoofing system synthesizes authentic GNSS signals, with code phases that induce a false position and time fix controlled by the spoofing system [1]. The false code phases are chosen in a way that ensures that the pseudorange residuals will be small. Meaconing is the recording and rebroadcasting of authentic GNSS signals. A meaconing system typically uses a single reception and a single (re-)transmission antenna. The victim receiver will then compute a position fix corresponding to the position of the meaconing system's reception antenna.

Spoofing detection can be performed in a number of different ways, for instance by analyzing if the characteristics of the received signal corresponds to those of the authentic satellite signals or by looking for evidence of interactions between authentic and spoofing signals. Spoofing detection algorithms can utilize information from a single receiver, multiple distributed antennas or receivers, an antenna array or complementary sensors (e.g. inertial sensors). An overview of different spoofing detection algorithms is provided in [1].

Many spoofing detection algorithms for scenarios with multiple receivers have been proposed using for example computed receiver positions as well as pseudorange or carrier phase measurements (see e.g. [4–10]). More specifically, double differences of pseudorange or carrier phase measurements have been used for spoofing detection [4, 9, 10]. Carrier phase double differences are used in [11] to classify spoofing signals based on the time invariance of the double differences in spoofing scenarios with one spoofing transmit antenna, which then are estimated and subtracted from the input signal, leaving authentic signals that can be used for Position, Velocity, and Time (PVT) computations. Spoofing signals are identified using multiple receivers and carrier phase double differences in [12] where both authentic and spoofed signals are acquired and tracked. The signals are divided into two groups based on navigation solution residual tests and carrier phase double differences are then used to identify the authentic and spoofing signal groups. Carrier phase double differences with multiple receivers are used to authenticate GNSS signals with a graph approach in [13]. A Generalized Likelihood Ratio Test (GLRT) is used on a linear model to find potential spoofing signals by testing the carrier phase double difference. Conceptually, a graph with Pseudo-Random Noises (PRNs) being vertices is constructed, where the vertices are connected if a GLRT favors the spoofing hypothesis. PRNs are used as identifiers for the satellites. The largest subset of connected PRNs are considered spoofed if it is of a certain size or larger, while the other are considered authentic. An overlap of authentic and

spoofed PRNs was not considered.

This work investigates the use of multiple GNSS receivers that exchange either pseudorange or carrier phase measurements in order to perform spoofing mitigation. The mitigation process consists of identifying measurements from spoofing signals based on double differences. It is based on the Master's thesis [14] and extends that work by considering more than two receivers. The algorithms presented here are inspired by the detection and mitigation algorithms based on multiple receivers presented above. An approach similar to [13] is adopted, but this work considers cases when the set of authentic and spoofed PRNs overlap. Furthermore, pseudoranges are used and the cases when the noise variances are unknown are evaluated.

II. Spoofing Mitigation Using Pseudorange or Carrier Phase Double Differences

Pseudorange and carrier phase measurements that may be generated by spoofing signals are first identified based on a binary hypothesis test that is applied to each individual double difference (measured over a time window). The GLRT is used to deal with the unknown parameters. These binary decisions are then combined to form a final decision on which pseudorange and carrier phase measurements originate from spoofing signals.

A. Assumptions

The following assumptions are made in this work:

(i) The spoofing system is assumed to utilize a single transmission antenna.

(ii) The receivers are assumed to be time synchronized (alternatively, the measurements can be interpolated to common time epochs).

(iii) The receivers are assumed to track both the authentic and spoofed signals for each satellite.

The two first ensure that the double-differences that are calculated based on pseudorange, or carrier phase, measurements belonging to two spoofing signals, will be time-invariant. The last that pseudorange and carrier phase measurements from both the authentic satellite signal and all spoofing signals are obtained for each satellite at all times. Finally, multipath propagation is not considered in this work.

B. Models of Authentic and Spoofed GNSS Measurements

Each spoofed signal corresponds to a falsified range d^k for each satellite k. These falsified ranges result in false pseudorange and carrier phase measurements in the receivers.

1) Pseudorange Measurement Model: Let $r_i^k[n]$ denote the geometric distance between receiver i and satellite k at time n. The distance between receiver i and the spoofing transmission antenna is denoted $\tilde{r}_i[n]$. The falsified range for satellite k at the transmission antenna of the spoofing system is $d^k[n]$, which can include for example atmospheric errors. Moreover, $\delta T_s[n]$ denotes a clock error in the spoofing system. The clock error in receiver i is denoted $\delta t_i[n]$ and the clock error in satellite k is denoted $\delta T^k[n]$.

Furthermore, let $I_i^k[n]$ and $\zeta_i^k[n]$ denote the ionospheric and tropospheric delay (in meter), respectively, between receiver i and satellite k. For receiver i and for each satellite signal k, the pseudorange measurement $\rho_i^k[n]$ can either be caused by an authentic or spoofed signal. This is modeled as (adapted from [9])

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

when the pseudorange measurement is generated by a spoofed signal, and

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

when it is generated by an authentic signal. The terms $\epsilon_i^k[n]$ and $\tilde{\epsilon}_i^k[n]$ are measurement noise, assumed to be Gaussian with zero mean similarly to [9]. The noise terms are assumed to be approximately equal, that is $\epsilon_i^k[n] \approx \tilde{\epsilon}_i^k[n]$, 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. Therefore, $\epsilon_i^k[n]$ is used to denote the noise term for both cases in this work.

2) Carrier Phase Measurement Model: Denote the carrier wavelength by λ and let N_i^k and $\tilde{N}_i^k$ be integers corresponding to the cycle ambiguities between receiver i and satellite k, for authentic and spoofed measurements respectively. The model for the carrier phase measurement $\phi_i^k[n]$ at time n for receiver i and satellite k is similar to the pseudorange measurements and can be expressed as

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

when the carrier phase measurement is generated by a spoofed signal[13], and

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

when it is generated by an authentic signal. The difference between the two models is analogous to the pseudorange case. The measurement errors, $\varepsilon_i^k[n]$ and $\tilde{\varepsilon}_i^k[n]$, are assumed to be Gaussian noise with zero mean. The variable $\varepsilon_i^k[n]$ is used to denote the noise term in both cases, based on the same assumptions as for the pseudorange measurements.

C. Identifying Spoofing Signals Based on Double Differences

Hypothesis testing is performed for either pseudorange or carrier phase double differences. 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 pseudorange 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 [9, 13]. The individual pseudoranges can be generated by either authentic or spoofed signals.

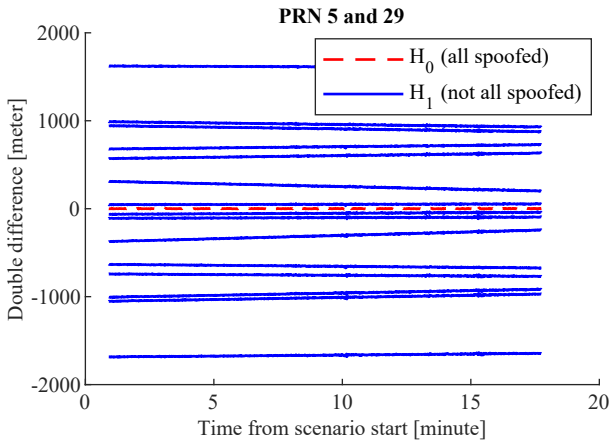

Fig. 1. Pseudorange double differences for a single satellite pair PRN 5 and 29 and two receivers separated by 100 meters.

The carrier phase single and double differences are computed analogously.

Next, consider two receivers, i and j, and a satellite pair k and l. Let null hypothesis, $\mathcal{H}_0$, be that all measurements (pseudoranges or carrier phases) in the double difference are computed from spoofed signals. The alternative hypothesis, $\mathcal{H}_1$, is then that at least one measurement in the double difference is not obtained from a spoofing signal.

1) Model of Pseudorange Double Differences: The double difference under $\mathcal{H}_0$ is

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

The double difference $\nabla\Delta\rho_{ij}^{kl}[n]$ under $\mathcal{H}_1$ is generally not zero mean, but it can be close to zero for some degenerative cases or for poorly separated receive antennas. Hence, no single expression exists for the double difference under $\mathcal{H}_1$ since it encompasses multiple cases. The double difference under $\mathcal{H}_1$ can have some offset and a component that changes over time.

A simple model for the double difference under $\mathcal{H}_1$ is that it is affine in time (for a sufficiently short time durations). The model is motivated by the examples of pseudorange double differences in Fig. 1 with two receivers separated by 100 meters (Scenario 1, see Sec. III) and satellite pair PRN 5 and 29. The double difference under $\mathcal{H}_0$ can be seen to be close to zero. In contrast, the differences under $\mathcal{H}_1$ are non-zero and some of them exhibit a slope. The pseudorange double differences are therefore modeled as

$$x_\rho[n] = \nabla\Delta\rho_{ij}^{kl}[n] = \begin{cases} w_\rho[n], & \text{under } \mathcal{H}_0, \\ A_\rho + B_\rho n + w_\rho[n], & \text{under } \mathcal{H}_1, \end{cases} \quad (1)$$

where $n = 1, 2, \ldots, N$. A_ρ and B_ρ are the unknown offset and slope coefficient, respectively. It follows from the measurement models that the noise $w_\rho[n] = \nabla\Delta\epsilon_{ij}^{kl}[n]$ is Gaussian noise with zero mean, and it is further assumed to be white. Its variance is denoted by σ_ρ^2 and N defines the length of the observation window.

The double difference can in some cases and for some satellite pairs be close to zero under $\mathcal{H}_1$. It will then be hard to distinguish $\mathcal{H}_1$ from $\mathcal{H}_0$. This happens e.g. for short distances between the receivers. Furthermore, the mean of the double difference under $\mathcal{H}_0$ could deviate from zero if the receiver measurements are not sufficiently time synchronized, thereby also making the identification harder.

The pseudorange double differences are collected over time in a vector

$$x_\rho \triangleq [\nabla\Delta\rho_{ij}^{kl}[1], \nabla\Delta\rho_{ij}^{kl}[2], \ldots, \nabla\Delta\rho_{ij}^{kl}[N]]^T.$$

The double differences, with slight abuse of notation, can then be written as

$$x_\rho = H_\rho\theta_\rho + w_\rho \quad (2)$$

where the observation matrix is

$$H_\rho \triangleq \begin{bmatrix} 1 & 1 & \ldots & 1 \\ 1 & 2 & \ldots & N \end{bmatrix}^T,$$

the parameter vector is $\theta_\rho = \theta_\rho^0 \triangleq [0, 0]^T$ under $\mathcal{H}_0$ and $\theta_\rho = \theta_\rho^1 \triangleq [A_\rho, B_\rho]^T$ under $\mathcal{H}_1$, and $w_\rho \triangleq [w_\rho[1], w_\rho[2], \ldots, w_\rho[N]]^T$.

2) Model of Carrier Phase Double Differences: The single differences and double differences of the carrier phase measurements are similar to the pseudorange equivalents. The carrier phase double difference is

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

under $\mathcal{H}_0$, where $\lambda\nabla\Delta N_{ij}^{kl}$ is assumed to be constant during the observation window, as in [13]. The double difference is modeled as a time-invariant offset plus noise under $\mathcal{H}_0$ and as affine, similarly to [13], under $\mathcal{H}_1$,

$$x_\phi[n] = \nabla\Delta\phi_{ij}^{kl}[n] = \begin{cases} A_\phi^0 + w_\phi[n], & \text{under } \mathcal{H}_0, \\ A_\phi^1 + B_\phi n + w_\phi[n], & \text{under } \mathcal{H}_1, \end{cases} \quad (3)$$

where $n = 1, 2, \ldots, N$. A_ϕ^0 and A_ϕ^1 are offsets and B_ϕ is a slope coefficient. It follows that the noise $w_\phi[n] = \nabla\Delta\varepsilon_{ij}^{kl}[n]$ is Gaussian noise with zero mean, and furthermore assumed white with variance σ_ϕ^2. There can be offsets A_ϕ^0 and A_ϕ^1 due to the cycle integer ambiguities that do not cancel when separate receivers are used. Examples of carrier phase double differences are shown in Fig. 2 for a single satellite pair where the receivers are separated by 100 meters (Scenario 1, see Sec. III). Double differences under $\mathcal{H}_1$ have in some cases weak trends, potentially making them more difficult to distinguish from $\mathcal{H}_0$. This can cause false spoofing detections.

The double differences are next collected in a vector

$$x_\phi \triangleq [\nabla\Delta\phi_{ij}^{kl}[1], \nabla\Delta\phi_{ij}^{kl}[2], \ldots, \nabla\Delta\phi_{ij}^{kl}[N]]^T.$$

It is then, again with slight abuse of notation, possible to write x_ϕ as

$$x_\phi = H_\phi\theta_\phi + w_\phi \quad (4)$$

where the observation matrix is $H_\phi \triangleq H_\rho$, the parameter vector is $\theta_\phi = \theta_\phi^0 \triangleq [A_\phi^0, 0]^T$ under $\mathcal{H}_0$ and $\theta_\phi = \theta_\phi^1 \triangleq [A_\phi^1, B_\phi]^T$ under $\mathcal{H}_1$, and $w_\phi \triangleq [w_\phi[1], w_\phi[2], \ldots, w_\phi[N]]^T$.

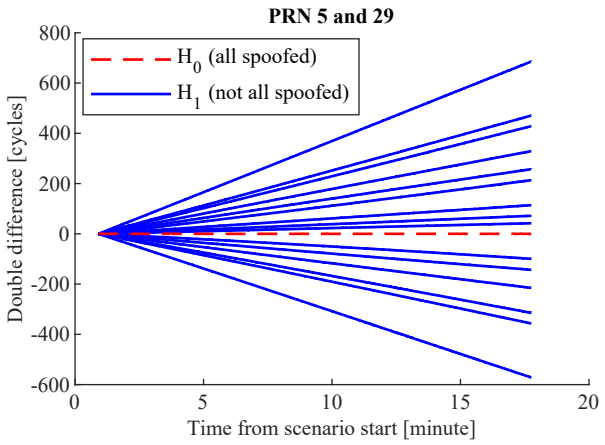

Fig. 2. Carrier phase double differences for a single satellite pair PRN 5 and 29 and two receivers separated by 100 meters. Each double difference has had its initial value removed to facilitate comparison.

D. Hypothesis Testing of Double Differences Using GLRTs

Based on the linear batch formulations (2) and (4), the hypotheses can be transformed to hypotheses on the parameter values instead

$$\begin{cases} C\theta = b, & \text{under } \mathcal{H}_0, \\ C\theta \neq b, & \text{under } \mathcal{H}_1, \end{cases} \tag{5}$$

where the pseudorange case follows directly as $C = I_2$ and $b = \theta_\rho^0 = [0, 0]^T$, whereas in the carrier phase $C = [0, 1]$ and $b = C\theta_\phi^0 = 0$ to ignore the effects of the unknown constant present in both hypotheses. In both cases, the noise levels are assumed known or unknown.

Given the formulation (5) a GLRT can be used to reject $\mathcal{H}_0$, see [15] details. Assuming the noise variance σ^2 known, the GRLT becomes

$$\frac{(C\hat{\theta} - b)^T [C(H^T H)^{-1} C^T]^{-1} (C\hat{\theta} - b)}{\sigma^2} \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \gamma \tag{6}$$

where $\hat{\theta} = (H^T H)^{-1} H^T x$ is the maximum likelihood estimate (MLE) of θ under $\mathcal{H}_1$ [15]. 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 (6) giving the desired probability of false alarm is [15]

$$\gamma = Q_{\chi_r^2}^{-1}(P_{\text{FA}}). \tag{7}$$

When the variance σ^2 is considered unknown, the GLRT instead becomes

$$\frac{N-p}{r} \frac{(C\hat{\theta} - b)^T [C(H^T H)^{-1} C^T]^{-1} (C\hat{\theta} - b)}{x^T (I - H(H^T H)^{-1} H^T) x} \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \gamma \tag{8}$$

where $\hat{\theta} = (H^T H)^{-1} H^T x$ is the MLE of θ under $\mathcal{H}_1$ [15]. 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 [15]

$$\gamma = Q_{F_{r,N-p}}^{-1}(P_{\text{FA}}). \tag{9}$$

Let **Test 1** be the GLRT based on the linear model (2) of pseudorange double differences when the noise variance σ_ρ^2 is known, and **Test 2** when the variance is unknown. They are given by (6) and (8), respectively, with $x = x_\rho$, $H = H_\rho$, $\sigma^2 = \sigma_\rho^2$, $C = I_2$ and $b = \begin{bmatrix} 0 & 0 \end{bmatrix}^T$. The theoretical threshold values are given by (7) and (9), respectively, for a false alarm rate P_{FA}. Note that Test 1 uses a fixed variance for both hypotheses while the variance is estimated under each hypothesis when Test 2 is used.

Next, let **Test 3** be the GLRT based on the linear model (4) of carrier phase double differences above when the variance is known and **Test 4** when the variance is unknown. They are given by (6) and (8), respectively, with $x = x_\phi$, $H = H_\phi$, $\sigma^2 = \sigma_\phi^2$, $C = \begin{bmatrix} 0 & 1 \end{bmatrix}$ and $b = 0$. The theoretical threshold values are given by (7) and (9), respectively, for a desired false alarm rate P_{FA}. The case of known variance is considered in [13] where the GLRT is used.

E. The Spoofing Mitigation Process Based on Double Difference Tests

The overall spoofing mitigation process for two receivers i and j, 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 $\Delta\phi_{ij}^k$. Each satellite gives rise to four single differences 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 indicated to be spoofed at least $K - 1$ times. The criterion is based on the assumption that the spoofing system transmits K or more spoofed satellite signals from a single transmission antenna. In this work, $K = 4$.
4) In case more than one measurement from a satellite remains at this stage, remove all measurements from that satellite. This is done since this method cannot decide which of them is correct if none of them is classified as being spoofed.
5) All remaining signals are considered authentic (not classified as spoofed), and should be used in the subsequent PVT computations.

F. Extension of the Spoofing Mitigation Process to More Than Two Receivers

A straightforward extension to use more than two receivers in the mitigation process is to simply perform the counting process for all combinations of receiver pairs and sum the count from each pairwise combination. This is done using the same process above, and increasing the count threshold for example by multiplying it with $R-1$ where R is the number of receivers.

Another approach is to set up a test that includes all receivers. Consider first the pseudorange measurements. The measurements are collected in a matrix

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

where R is the number of receivers, for a satellite pair k and l. X is then modeled as

$$X = \bar{H}\Theta + W \tag{10}$$

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

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

That is, the double differences are modeled as straight lines with slopes B_{ij}^{kl} and offsets A_{ij}^{kl}. Note that receiver 1 is used, without loss of generality, as a reference here.

The measurement model given by (10) is next vectorized as

$$\begin{aligned} x_{\text{vec}} &\triangleq \text{vec}(X^T) = \text{vec}(\Theta^T\bar{H}^T) + \text{vec}(W^T) \\ &= (\bar{H} \otimes I_{R-1})\text{vec}(\Theta^T) + \text{vec}(W^T) \\ &= H_{\text{vec}}\theta_{\text{vec}} + w_{\text{vec}} \end{aligned} \tag{11}$$

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.

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 time (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

$$P = \sigma_{\text{vec}}^2\bar{P}$$

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

$$\Omega = I_N \otimes (\sigma_{\text{vec}}^2\bar{P}) = \sigma_{\text{vec}}^2(I_N \otimes \bar{P}) = \sigma_{\text{vec}}^2\bar{\Omega}$$

where $\bar{\Omega} \triangleq (I_N \otimes \bar{P})$. The matrix $\bar{P}$ is positive definite and thus have 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 is possible to pre-whiten (11) using the square root $\bar{\Omega}^{1/2}$, yielding

$$x'_{\text{vec}} = H'_{\text{vec}}\theta_{\text{vec}} + w'_{\text{vec}} \tag{12}$$

where $x'_{\text{vec}} \triangleq \bar{\Omega}^{1/2}x_{\text{vec}}$, $H'_{\text{vec}} \triangleq \bar{\Omega}^{1/2}H_{\text{vec}}$ and $w'_{\text{vec}} \triangleq \bar{\Omega}^{1/2}w_{\text{vec}}$ with covariance $\text{cov}(w'_{\text{vec}}) = \sigma_{\text{vec}}^2 I$ [15].

The hypothesis test (5) is then used on the pre-whitened model (12), with $C = I_{2(R-1)}$ and $b = 0_{2(R-1)\times 1}$. $\mathcal{H}_0$ denotes that all measurements in the test are from spoofing signals and $\mathcal{H}_1 = \neg\mathcal{H}_0$. Tests (6) or (8) can then be used, assuming that the noise variance is known or unknown respectively. A test can, analogously, be created for the carrier phase measurements, but instead using $C = \begin{bmatrix} 0_{(R-1)\times(R-1)} & I_{R-1} \end{bmatrix}$ and $b = 0_{(R-1)\times 1}$. The mitigation process is then performed in the same way as described in Sec. II-E for two receivers.

III. Implementation and Tests

This section briefly describes how the algorithms were implemented and evaluated. For more details on the implementation, see [14]. An overview of the implementation is shown in Fig. 3.

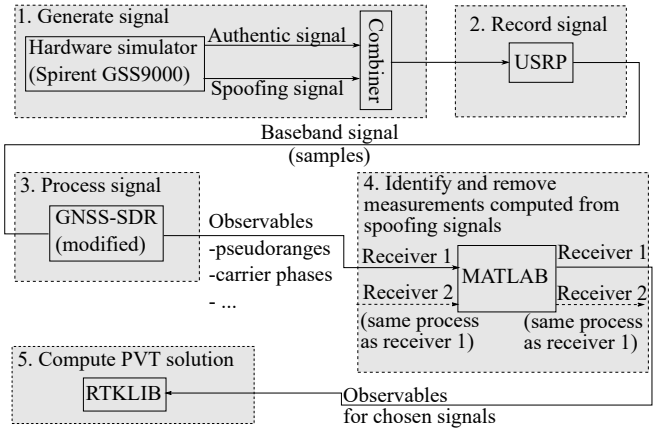

Fig. 3. Overview of the implementation.

A. Data Generation and Collection

Authentic GPS L1 C/A and spoofing signals were generated using a Spirent GSS9000 GNSS Signal Generator. The signals were recorded using a USRP[1] (Universal Software Radio Peripheral) and saved as complex baseband samples at $4\,\text{MHz}$.

The simulation was set up to mimic a meaconing attack, but noise was not amplified as it would be in a real-world meaconing attack. Thus, the simulated spoofing attack can also be seen as self-consistent spoofing. Several different receiver positions were simulated and then combined into different scenarios.

B. Modification of GNSS-SDR

The spoofing mitigation algorithms require the use of multiple receivers that track both authentic and spoofed signals. The open source software defined GNSS receiver GNSS-SDR[2] was modified and used for this work. The GNSS-SDR project is described in [16]. GNSS-SDR was modified to acquire and track extra signals (correlation peaks) for each satellite, in addition to the strongest signal. The software saves internal data such as pseudoranges and carrier phases in MATLAB data files.

C. Implementation of Algorithms and Position Computation

The spoofing mitigation algorithms were implemented in MATLAB and they use the observables (pseudoranges and carrier phases) obtained from the modified GNSS-SDR. The algorithm removes observables from identified spoofing signals, then forwards the remaining measurements to the Real-Time Kinematic Library[3] (RTKLIB) for subsequent PVT computations.

The measurements from GNSS-SDR have time stamps that are initial receiver time estimates. GNSS-SDR sets this receiver time common for all channels, based on a reference satellite. These time estimates are then used in MATLAB to synchronize the measurements from the separate receiver runs.

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

[2]See https://gnss-sdr.org/. Version 0.0.10 of GNSS-SDR was used.

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

TABLE I
GLOBAL SCENARIO PARAMETERS FOR THE SIMULATIONS.

Parameter	Value
Start time	01-Jul-2012 20:00:00 UTC
Simulation time	20 min
Base position[a]	$59^\circ, 17^\circ$, 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.

TABLE II
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
Scenario 1	1,2	100	SE-NW
Scenario 2	3,4	100	SW-NE
Scenario 3	1,5	1	SE-NW
Scenario 4	1,6	5	SE-NW
Scenario 5	1,7	10	SE-NW
Scenario 6	1,8	20	SE-NW
Scenario 7	1,9	35	SE-NW
Scenario 8	1,10	50	SE-NW

Position computation on the measurements remaining after the mitigation process is possible using RTKLIB, yielding the correct receiver positions (close to correct positions on average). This was verified in the cases when the authentic measurements were successfully extracted. The position was also computed using the inverse selection of signals, which yielded the position of the meaconing system's reception antenna. This was performed for all simulations to verify that both the authentic and the spoofing signals are correct and produce reasonable positions.

D. Simulated Scenarios

Only scenarios with stationary receiver and spoofer positions were generated. The spoofing attacks were simulated for different receiver positions using the parameters specified in Table I. A delay corresponding to 400 meters (distance equivalent of the propagation delay) was added to the spoofed signals in addition to the spoofing signal propagation delay. This delay simulates a processing delay and delay between the reception and transmission antennas of the meaconing system. Both authentic and spoofing signals are present from the beginning of the scenarios.

The receiver positions are shown in Fig. 4 (denoted Rx_i) together with the position of the meaconer. The simulated receiver positions were combined into different scenarios, see Table II, to investigate the impact of the geometry and distance between receivers. Two to four receivers were combined as specified in Table III. The power of the signals were simulated to correspond to the nominal signal power at the surface of the earth. The authentic and spoofing signals were generated with equal powers.

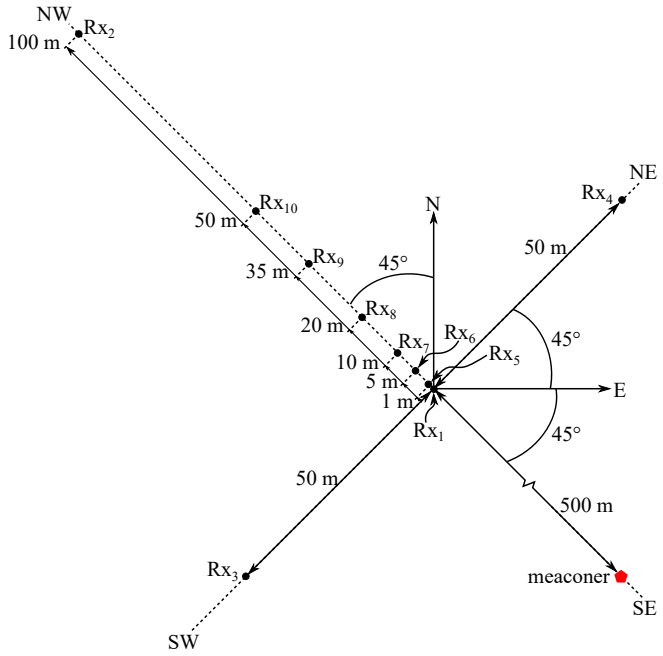

Fig. 4. Simulated receiver positions and position of meaconer.

TABLE III
COMBINATION OF MULTIPLE RECEIVERS. THE REFERENCE RECEIVER IS UNDERLINED.

Distance (m)	**Receivers**	**Combinations**
5	1,6,7	$\{1,\underline{6}\},\{\underline{6},7\},\{1,\underline{6},7\}$
50	1,3,4,10	$\{\underline{1},4\},\{\underline{1},10\},\{\underline{1},4,10\},\ldots$ $\{\underline{1},3,4,10\}$

IV. RESULTS

The spoofing mitigation methods described in Sec. II are evaluated next using the implementation and simulation set-up described in Sec. III. The modified GNSS-SDR tracked authentic and spoofed signals for 7 satellites in these simulations.

A. Spoofing Mitigation Using Pseudoranges

The pseudorange and carrier phase measurements are taken from GNSS-SDR at a rate of 50 Hz. The sampling rate was decreased to 1 Hz (by using every 50th measurement) to make samples of the double differences less correlated for different time instances and to correspond to a more realistic scenario.

Spoofing mitigation using pseudorange double differences with Test 1 (GLRT assuming known noise variance given by (6)) and Test 2 (GLRT assuming unknown noise variance given by (8)) worked well using the theoretical thresholds given by (7) and (9). An average variance from the different scenarios was computed in advanced for the double differences under $\mathcal{H}_0$ and used in Test 1. The thresholds are set using a probability of false alarm of 1 % as default.

Initial evaluations were performed to compare Tests 1 and 2. The performance of Test 1 did not provide consistently better results for all scenarios compared to Test 2 when a fixed value of the known variance was used. Note that the variance of the double differences can vary for different scenarios. Using a test statistic that assumes the variance to be known might be difficult to accomplish in practice. Thus, Test 2 that assumes the variance to be unknown will be used for the evaluations from here on.

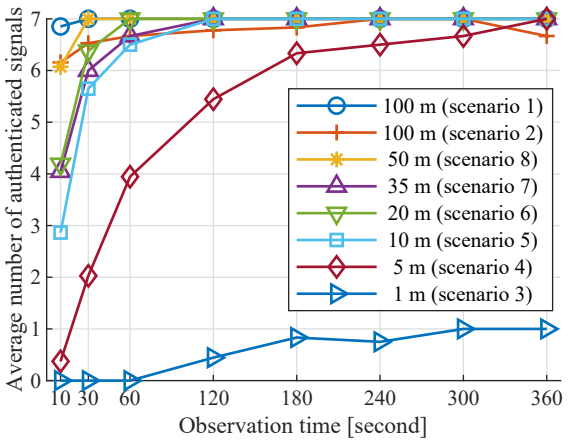

Fig. 5. The performance of test 2 using pseudoranges as a function of observation time for Scenarios 1–8. Average number of correctly authenticated signals (of total 7).

1) Different Observation Window Lengths and Baseline Lengths: Different observation lengths are evaluated next for Test 2. Different observation lengths are evaluated by dividing the scenarios into observation windows with the appropriate length, and applying the spoofing mitigation algorithms. The average number of correctly authenticated signals (signals left after the mitigation process that are authentic) is computed over these time windows. Spoofed signals left after the mitigation process that are spoofed are incorrectly authenticated. The number of correctly authenticated signals should, in theory, improve with increasing observation length. Fig. 5 shows the performance of Test 2 for different observation lengths. The performance is measured as the average number of correctly authenticated signals as a function of the observation length. Most signals, on average more than 6 of 7, are correctly authenticated within one minute for distances between the receivers larger than, or equal to, 10 meters, using the pseudorange double difference test. The average number of incorrectly authenticated signals were zero in all cases, except for Scenario 4 (5 meter receiver distance) and for the shortest observation window of 10 seconds for which it was 0.0091. It can be seen that the performance improves for longer observation windows in most cases. The slight decrease in performance in Scenario 2 for the longest observation interval could, for example, be caused by random variations or if the time synchronization error of the two receivers was slightly larger in that scenario, which could be noticed at longer observation intervals.

It is evident that spoofing mitigation based on pseudoranges performs poorly for short baselines. Shorter baselines require longer identification time, but longer observation windows

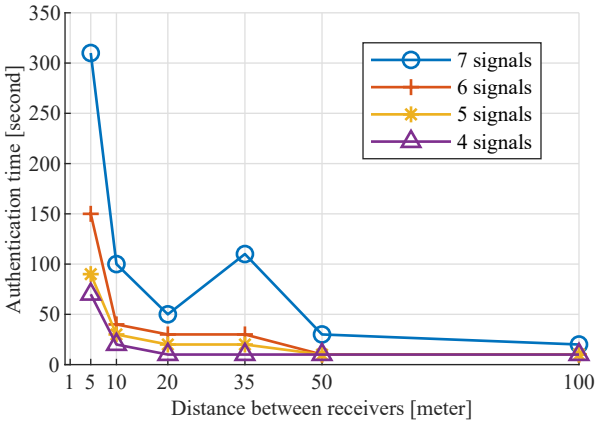

Fig. 6. Authentication time for Test 2 using pseudoranges as a function of the distance between the receivers for Scenario 1 and 3–8. The number of tracked satellites were 7.

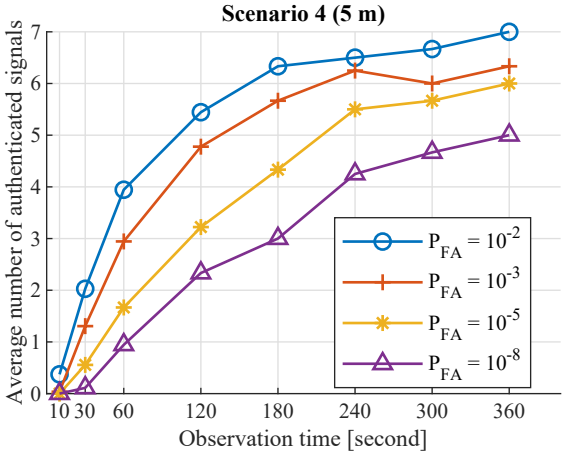

Fig. 7. Performance of Test 2 for Scenario 4 shown for different probability of false alarm. Average number of correctly authenticated signals (of total 7) as a function of observation time.

does not necessarily help for distances shorter than 5 meters. It can also be seen in Fig. 5 that longer distance between the receivers enables faster authentication of most of the signals. However, there is a clear decrease in performance for the 35 meter distance (Scenario 7) compared to Scenario 6 (20 meters), which could be caused by the receiver to satellite geometry in that particular case. More pseudorange double differences under $\mathcal{H}_1$ are close to zero in Scenario 7 compared to Scenario 6. It is also clear that the performance in Scenario 1 is better than in Scenario 2. This means that the performance could also depend on the geometry of receivers and spoofing system.

The authentication time is shown as a function of the distance between the receivers in Fig. 6 for Test 2. It was computed as the shortest observation length that yielded an average of 7, 6, 5, and 4 correctly authenticated signals (100 %, 86 %, 71 %, and 57 % of the signals, respectively) for each respective scenario (distance). Observation windows between 10 seconds and 360 seconds were evaluated in increments of 10 seconds. Note that no data points are available for the 1 meter distance (Scenario 3). That particular distance is too short for reliable authentication using pseudoranges. Scenario 2 was excluded in this evaluation. It can again be seen that the distance 35 meters (Scenario 7) has worse performance than what is obtained at 20 meters.

2) The Effect of the False Alarm Probability: The probability of false alarm was varied, resulting in different thresholds, and evaluated for Test 2 for Scenario 4, see Fig. 7. The number of incorrectly authenticated signals was zero in all cases except for $P_{\text{FA}} = 1\,\%$ and the shortest observation time 10 seconds where it was 0.0091. It can be seen that the required observation time is reduced when accepting higher probability of false alarm. The other scenarios display the same property.

3) Spoofing Signals With Different Power Levels: The receiver positions Rx_1 and Rx_{10} (receiver positions 1 and 10, separated by 50 meter) were also simulated for different power levels of the spoofing signals. The power level is specified relative to the authentic L1 C/A signals. The following power levels were simulated: -3 dB, $+3$ dB, $+10$ dB and $+20$ dB.

The unmodified GNSS-SDR was first evaluated on the simulated signals with spoofing signals having different power levels. The unmodified GNSS-SDR computed the correct position when the spoofing signal power level was -3 dB lower than the authentic L1 C/A signal. It did not compute any position in most cases when the spoofing signals have the same strength as the authentic signals. This is likely caused by the receiver having acquired a mix of spoofed and authentic signals. These signals form an inconsistent set of measurements (pseudoranges). The unmodified GNSS-SDR computed the incorrect position (the position of the meaconer) for power levels $+3$ dB, $+10$ dB and $+20$ dB.

Next, the modified GNSS-SDR was used to evaluate Test 2 with the different power levels. The probability of false alarm was set to $0.1\,\%$ in these evaluations. Evaluations were performed for observation windows between 30 seconds and 360 seconds. The performance was noticeably affected only for the $+10$ dB and $+20$ dB cases and the shortest observation interval. The average number of correctly authenticated signals was around 7 (of total 7) for all cases except the shortest observation interval 30 seconds with $+10$ dB and $+20$ dB spoofing signals where it was around 6. The number of incorrectly authenticated signals was zero for all power levels and all observation intervals. Note that these spoofing attacks that were simulated are slightly easier for the algorithms to handle compared to a real meaconing attack that would also amplify noise. Amplified noise likely further increase the errors in the pseudorange measurements.

B. Spoofing Mitigation Using Carrier Phases

The spoofing mitigation algorithms were evaluated on the carrier phase double differences using Test 3 (GLRT assuming known noise variance given by (6)) and Test 4 (GLRT assuming unknown noise variance given by (8)). The theoretical

threshold was evaluated first, using different probabilities of false alarm. The theoretical threshold did not work well. This is probably due to the carrier phase double differences under $\mathcal{H}_0$ having small trends in some cases, which likely was caused by receiver time synchronization errors. The results in [9] indicate that spoofing detection based on carrier phase double differences requires more accurate synchronization than using pseudorange double differences. The distribution of the test statistics under $\mathcal{H}_0$ versus $\mathcal{H}_1$ is however separated enough that detection should be possible, but the threshold has to be set in another way. The threshold was instead set empirically by investigating the distribution of the test statistics under $\mathcal{H}_0$ and setting the threshold to yield a false alarm rate of $1\,\%$. Note that the theoretical threshold in (7) for the test statistic assuming known variance does not depend on the length of the observation window, while the threshold in (9) for the test statistic estimating the variance does depend on the length of the observation window. Note that the theoretical thresholds might work for better time synchronization of the measurements, see e.g. [13].

The variance can be set to one for Test 3, since the threshold is set empirically. This empirically set threshold is kept the same for all scenarios and different observation lengths when Test 3 is used. The threshold for Test 4 was also set empirically, but individually for each observation length.

The number of correctly authenticated signals as a function of observation time for Scenarios 1–8 using Tests 3 and 4 is shown in Fig. 8 and Fig. 9, respectively. The number of incorrectly authenticated signals were zero for all scenarios and all observation lengths. The performance of Test 4 is slightly more consistent than for Tests 3, and Test 4 can authenticate the signals faster in most cases. This could be explained by the fact that the threshold for Test 4 was set for each length of observation window individually. Hence, Test 4 can have better performance for each window considering all scenarios. Test 3 uses a threshold that has to work for all scenarios and all lengths of observation windows. The performance of Test 3 is therefore more varied and less consistent, which can be seen for the longer observation lengths.

The same trends apply here as for the pseudoranges. A longer observation window generally means better performance, that is faster authentication of signals and more signals authenticated faster. The trend is also that larger distances between the receivers yield better performance. The decreases in performance for the longer observation intervals can be due to that the slight trends of some of the double differences under $\mathcal{H}_0$ are more noticeable for longer observation windows. These trends can be more noticeable in some scenarios. The model of the carrier phase double differences as being straight lines with an offset under $\mathcal{H}_1$ is also less accurate for longer observation lengths, which can negatively influence the performance of the test. However, Test 3 is better than Test 4 at authenticating signals in Scenario 3 for longer observation intervals. The fixed threshold for Test 3 performs well in Scenario 3 seemingly at the cost of worse performance for some of the other scenarios for the longer observation windows. This is the result of setting the threshold for Test 3 to accommodate all observation windows and all scenarios, which partly favors Scenario 3 here.

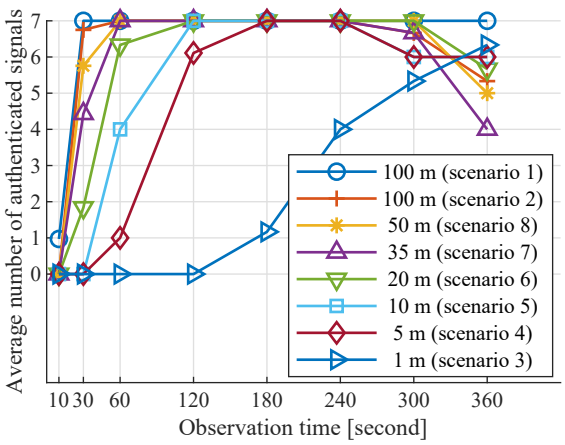

Fig. 8. Average number of correctly authenticated signals as a function of observation time for Scenarios 1–8 using Test 3 (carrier phases).

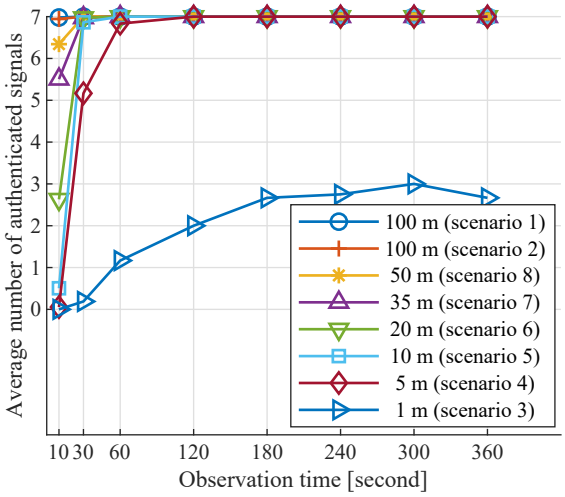

Fig. 9. Average number of correctly authenticated signals as a function of observation time for Scenarios 1–8 using Test 4 (carrier phases).

C. Spoofing Mitigation With Two and More Receivers

The extended algorithms described in Sec. II-F are next evaluated for the 5 meter and 50 meter scenarios according to Table III. The performance in these two cases is shown in Fig. 10 and 11 where alt. 1 and 2 refer to the first (sum everything together) and second (new extended model) proposed extension, respectively, in Sec. II-F. The number of incorrectly authenticated signals was zero for observation lengths of 30 seconds and longer, and less than 0.03 in the other cases for the 5 meter scenario. No spoofing signals were incorrectly authenticated in the 50 meter scenario. The evaluations were performed for pseudoranges only. The theoretical thresholds were used with $P_{\text{FA}} = 1\,\%$ and variance was assumed to be unknown.

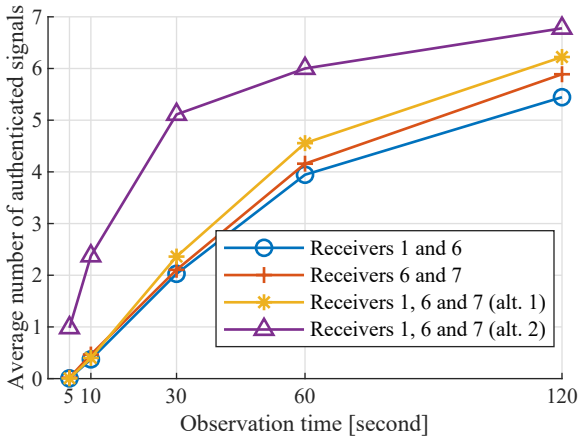

Fig. 10. Average number of correctly authenticated signals as a function of observation time. The alternatives alt. 1 and 2 refer to the first (sum everything together) and second (new extended model) proposed extension, respectively. Scenario with receivers 1, 6 and 7 (5 meter distances). Receiver 6 is used as reference.

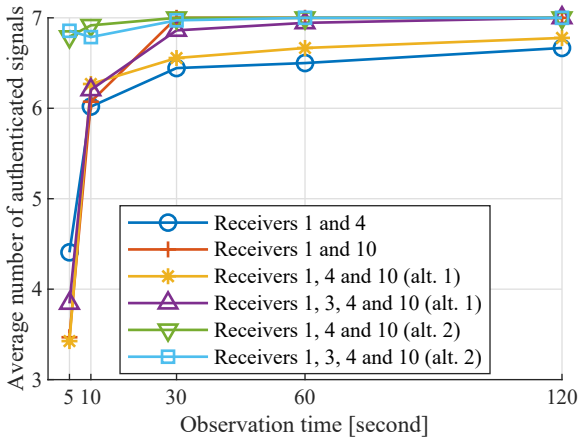

Fig. 11. Average number of correctly authenticated signals as a function of observation time. The alternatives alt. 1 and 2 refer to the first (sum everything together) and second (new extended model) proposed extension, respectively. Scenario with receivers 1, 3, 4 and 10 (50 meter distances). Receiver 1 is used as reference.

The performance can be improved by using more than two receivers, considering alt. 2. However, the results are more mixed with alt. 1. There is a slight improvement in Fig. 10, but not in Fig. 11 where the receiver combination $\{1, 4, 10\}$ is worse than just $\{1, 10\}$, for example.

V. Concluding Remarks

Four novel algorithms to mitigate GNSS spoofing have been derived based on double differences of pseudorange or carrier phase measurements from multiple receivers with known or unknown noise levels. Even strong spoofing signals can be mitigated by utilizing these algorithms, provided that the noise levels can be accurately estimated. The performance of the spoofing mitigation algorithms improve as the distance between the receivers increases. Using pseudorange double differences, spoofing signals can be reliably mitigated for receiver distances larger than five meters. Larger separation and longer observation windows allows for more accurate identification of the spoofing signals. By increasing the number of cooperating receivers the mitigation performance is improved, particularly for scenarios with short receiver separations.

In contrast, spoofing mitigation is possible with receiver separations well below five meters when utilizing the carrier phase double differences. However, a potential drawback is that this approach requires a more accurate time synchronization compared to the pseudorange double difference algorithm.

Future work should investigate improved methods for synchronizing the measurements from separate receivers, especially if carrier phase double differences are to be used. The spoofing mitigation should also be evaluated with real GNSS data to verify that the algorithms and implementation work with actual spoofing attacks.

References

[1] M. L. Psiaki and T. E. Humphreys, "GNSS spoofing and detection," *Proc. IEEE*, vol. 104, no. 6, pp. 1258–1270, Jun. 2016.

[2] 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 *Proc21st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS)*, Savannah, GA, Sep. 2008, pp. 2314–2325.

[3] "Above us only stars – Exposing GPS spoofing in Russia and Syria," C4ADS report, Apr. 2019.

[4] E. Axell, M. Alexandersson, and T. Lindgren, "Results on GNSS meaconing detection with multiple COTS receivers," in *Proc. International Conference on Localization and GNSS (ICL-GNSS)*, Gothenburg, Sweden, Jun. 2015, pp. 1–6.

[5] E. Axell, E. G. Larsson, and D. Persson, "GNSS spoofing detection using multiple mobile COTS receivers," in *Proc. IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Brisbane, QLD, Apr. 2015, pp. 3192–3196.

[6] P. F. Swaszek and R. J. Hartnett, "A multiple COTS receiver GNSS spoof detector – extensions," in *Proc. International Technical Meeting of The Institute of Navigation*, San Diego, CA, Jan. 2014, pp. 316–326.

[7] ——, "Spoof detection using multiple COTS receivers in safety critical applications," in *Pro. 26th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+)*, Nashville, TN, Sep. 2013, pp. 2921–2930.

[8] D. S. Radin, P. F. Swaszek, K. C. Seals, and R. J. Hartnett, "GNSS spoof detection based on pseudoranges from multiple receivers," in *Proc. International Technical Meeting of The Institute of Navigation*, Dana Point, CA, Jan. 2015, pp. 657–671.

[9] F. Wang, H. Li, and M. Lu, "GNSS spoofing detection based on unsynchronized double-antenna measurements," vol. 6, pp. 31 203–31 212, 2018.

[10] J. Wen, H. Li, Z. Wang, and M. Lu, "Spoofing discrimination using multiple independent receivers based on code-based pseudorange measurements," in *Proc. 32nd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+)*, Miami, FL, Sep. 2019, pp. 3892–3903.

[11] A. Jafarnia-Jahromi, A. Broumandan, S. Daneshmand, N. Sokhandan, and G. Lachapelle, "A double antenna approach toward detection, classification and mitigation of GNSS structural interference," in *Proc. 6th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC)*, Noordwijk, Netherlands, Dec. 2014.

[12] S.-H. Seo, B.-H. Lee, S.-H. Im, G.-I. Jee, and K.-S. Kim, "Efficient spoofing identification using baseline vector information of multiple receivers," *GPS Solutions*, vol. 22, no. 115, 2018.

[13] A. J. Jahromi, A. Broumandan, and G. Lachapelle, "GNSS signal authenticity verification using carrier phase measurements with multiple receivers," in *Proc. 8th ESA Workshop on Satellite Navigation Technolo-*

gies and European Workshop on GNSS Signals and Signal Processing (NAVITEC), Noordwijk, Netherlands, Dec. 2016, pp. 1–11.

[14] N. Stenberg, "Spoofing mitigation using multiple GNSS-receivers," Master's thesis, Department of Electrical Engineering, Linköping University, Linköping, Sweden, 2019. [Online]. Available: http://urn.kb.se/resolve?urn=urn:nbn:se:liu:diva-158461

[15] S. M. Kay, *Fundamentals of Statistical Signal Processing, Volume II: Detection Theory*. Prentice-Hall PTR, 1998.

[16] C. Fernández-Prades, J. Arribas, P. Closas, C. Avilés, and L. Esteve, "GNSS-SDR: an open source tool for researchers and developers," in *Proc. 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS)*, Portland, OR, Sep. 2011, pp. 780–794.