Optimization and performance of multi-criteria collaborative integrity control in degraded GNSS environments

Victor Vince, Dominique Heurguier, Alexandre Vervisch-Picois, Jose Rubio-Hernan

Optimization and Performance of Multi-Criteria Collaborative Integrity Control in Degraded GNSS Environments

Victor Vince[1,2,*,†], Dominique Heurguier[2,†], Alexandre VERVISCH-PICOIS[2,†] and Jose Manuel RUBIO HERNAN[2,†]

[1]SAMOVAR, Telecom SudParis, Institut Polytechnique de Paris, Palaiseau, France
[2]Thales SIX, Gennevilliers, France

Abstract

This study aims to establish the performance of a multi-criteria collaborative integrity control in the presence of GNSS spoofing. The plurality of criteria means that multiple sources of information are used simultaneously to determine whether or not the position of the receivers is degraded by a GNSS attack. By using the residuals of the PVT (position, velocity, time) estimation and the C/N_0 ratio (expressed in dB-Hz), a robust integrity control can be obtained with all the data used. The main strength of this integrity control lies in the collaboration between receivers through comparison and sharing of information. Additionally, it only adds a software layer to the system, and no additional hardware is required for this method. It works equally well with a limited number of receivers as it does with a large number of receivers.

Keywords

GNSS, Real Data, Spoofing, Jamming, Collaboratives Solutions, Hybridation, Integrity Monitoring, Covariance Estimation

1. Introduction

This study builds upon previous work on CERIM (Collaboration-Enhanced Receiver Integrity Monitoring), which is an extension of RAIM (Receiver Autonomous Integrity Monitoring) in a collective manner. This collaborative method uses residuals from the last iteration to obtain the best PVT estimation of the receiver through iterative convergence methods (Gauss-Newton). It is important to note that these residuals significantly increase when inconsistency in the data appears, and this inconsistency can be detected by multiple receivers. These inconsistencies can be caused by spoofing and jamming. Spoofing is a type of attack in which an adversary manipulates a Global Navigation Satellite System (GNSS) receiver by broadcasting counterfeit signals that closely resemble legitimate GNSS signals. The goal is to deceive the victim receiver into interpreting the fraudulent signals as authentic, resulting in incorrect position data, incorrect clock offset, or both. This attack can mislead navigation systems, causing serious consequences for applications relying on accurate positioning. Jamming involves the deliberate transmission of interfering signals that disrupt the communication between a GNSS receiver and the satellite constellation, leading to signal loss. This is commonly referred to as a denial-of-service (DoS) attack. In cases where spoofing is accompanied by jamming, the receiver may enter a "search" phase in an attempt to regain signal lock, which makes it particularly vulnerable to the spoofing attack. In this scenario, jamming acts as a facilitator, helping the spoofing attack to succeed by increasing the receiver's reliance on false signals. The residuals come from several PVT data estimates, including residuals from pseudo-range estimation and Doppler estimation, which are essential for evaluating the

WIPHAL'25: Work-in-Progress in Hardware and Software for Location Computation June 10–12, 2025, Rome, Italy
*Corresponding author.
†These authors contributed equally.
victor.vince@thalesgroup.com (V. Vince); dominique.heurguier@thalesgroup.com (D. Heurguier); alexandre.vervisch-picois@telecom-sudparis.eu (A. VERVISCH-PICOIS); jose.rubio-hernan@telecom-sudparis.eu (J. M. R. HERNAN)
0009-0005-9139-1514 (V. Vince); 0000-0001-5577-5047 (A. VERVISCH-PICOIS); 0000-0001-9778-8049 (J. M. R. HERNAN)

receiver's speed. Two monitoring statistics are formed on these two residual vectors. A third monitoring statistic is based on the C/N_0 ratio, which is an excellent indicator of noise level and received signal power evolution by the receivers. This parameter provides a very effective indicator, especially for GNSS jamming detection. This monitoring statistic informs us of any significant degradation of GNSS signals in an area where the monitored group of receivers is evolving. A fourth monitoring can also be added: the monitoring of the receiver clock drift. Indeed, according to [1], unless the spoofing attack involves "time monitoring," there is almost always a detectable jump in the calculated clock drift when the receiver is a victim of a spoofing attack.

First, we will examine the formation of monitoring statistics based on residuals and their behavior in response to common and sophisticated spoofing attacks. Then, we will analyze the reaction of C/N_0 ratios during jamming and spoofing attacks. Finally, we will conclude on the different scenarios that allow for the implementation of this system.

2. CERIM Methodology

Before presenting the CERIM methodology, it is useful to review related studies on collaborative integrity monitoring in GNSS systems, particularly for spoofing and jamming detection. One approach, detailed by [2], uses positioning-based detection: if receivers cannot achieve precise alignment, an alarm is triggered. Another relevant study by [3] focuses on collaborative RAIM, where multiple receivers share residuals to enhance the detection of spoofing. This article contributes to the effort of pooling information between receivers to enhance the detection of attacks and inconsistencies, which could have unprecedented consequences on critical systems.

CERIM is a collaborative method designed to establish a monitoring statistic that highlights position drifts resulting from natural technical errors. The main strength of CERIM lies in the fact that it requires no bulky infrastructure, except for a communication link between each receiver and a centralization of information to be operational. This feature allows CERIM to provide a robust integrity control, particularly in the presence of receivers close to each other evolving in a complex environment with multiple reflections and obstructions [4], [5]. Essentially, CERIM is an extension of RAIM [6], which has demonstrated its usefulness for detecting satellite clock failures, but remains vulnerable to certain attacks, such as coherent spoofing [7]. Coherent spoofing is a form of spoofing that induces a consistent false position after calculation, without causing a significant residual error.

RAIM and CERIM use calculation residuals to ensure the validity of positioning calculations. These residuals significantly increase in case of errors, allowing a monitoring statistic to be established over time. When calculating a position using pseudo-distances provided by the receiver, the method used aims to determine the position that best satisfies the observed data. The uncertainties inherent in measurements result in residuals in the solution of an overdetermined system of equations because this solution represents the best compromise with respect to the entire set of equations. If one of the equations presents measurements that deviate significantly from this compromise solution, it will be reflected in the residual and, consequently, in the associated monitoring curve. When the receiver captures signals from at least five satellites, the problem becomes overdetermined, allowing residuals to be obtained. In this study, these residuals concern both pseudo-distances and calculated velocities.

The residuals in satellite space are interdependent because subtracting theoretical measurements based on a common estimation of the solution introduces algebraic coupling. The residual vector $\mathbf{r}_{global}$ is as long as two times the number of satellites L_n visible by receiver n. The method used is a least squares estimation [8]. $\mathbf{H}$ corresponds to the Jacobian matrix of dimension $\mathbb{R}^{(L_n \times 2) \times 4}$.

$$\Delta \mathbf{x} = \left(\mathbf{H}^T \mathbf{H}\right)^{-1} \mathbf{H}^T \Delta \boldsymbol{\rho} \tag{1}$$

In this study, the 8 parameters constituting PVT are estimated jointly. This allows for the simultaneous estimation of the position vector $[x, y, z]$, the velocity vector $[v_x, v_y, v_z]$, the clock bias t, and the clock drift $\dot{t}$. The residual vector, extracted after the joint calculation of these eight parameters, has a dimension of $\mathbb{R}^{L_n \times 2}$ because the method used requires redundancy in the pseudorange data to

accurately estimate the receiver's velocity.

The global residual vector is decomposed into two sub-vectors:

$$\mathbf{r}_{global} = \mathbf{r}_{psd-rg} + \mathbf{r}_{dplr} \tag{2}$$

These sub-vectors have dimensions equal to $\mathbb{R}^{L_n}$.

In this study, we extend CERIM to Doppler residuals. This monitoring of Doppler frequency estimation residuals ($\mathbf{r}_{dplr}$) will be more precise because it is a measure of the relative velocity between the satellite and the receiver, derived from the frequency shift of the received signal. The Doppler frequency results from the demodulation of the signal's carrier, which is less sensitive to the environment (noise and multipath), thereby reducing the impact of certain errors. Errors affecting the Doppler frequency are related to the temporal drift of pseudorange errors. Therefore, the CERIM statistic, established from Doppler residuals, proves to be particularly sensitive, especially in cases of attacks lacking coherence in Doppler signal estimation. Indeed, it is challenging to make a spoofing attack coherent at the Doppler signal level. While it is theoretically possible to make such an attack coherent, it is much more complex in practice [9].

2.1. Parity algorithm

These two sub-vectors of residuals are expressed in the satellite space $\mathbf{r} \in \mathbb{R}^{L_n}$. Given that the residuals are constrained to be orthogonal to the four columns of the Jacobian matrix, the residuals of the sub-vectors $\mathbf{r}_{psd-rg}$ and $\mathbf{r}_{dplr}$ are not independent. This redundancy leads to a degenerate non-invertible covariance matrix of the residuals. Therefore, this representation of the residual vector has the disadvantage of introducing an algebraic dependency between the residuals by mixing the measurements necessary for the solution calculation and the redundant measurements. It is then wise to transform the residuals into an alternative form that eliminates redundancy by considering a space, called the parity space [10], where the relationships (parities) are independent of the unknown solution. This alternative form of the residual vector is generally called the parity vector $\mathbf{p}_n$.

$$\mathbf{p}_n = \mathbf{N}_n^T \, \mathbf{r}_n \tag{3}$$

where $\mathbf{N}_n^T$ is the null space matrix of the Jacobian matrix $\mathbf{H}_n$ such that $\mathbf{N}_n^T \mathbf{H}_n = 0$. It has a dimension of $\mathbb{R}^{L_n \times (L_n - 4)}$.

Once the two sub-vectors are in the parity space: $\mathbf{p}_{n_{psd-rg}}$ and $\mathbf{p}_{n_{dplr}}$, both with dimensions $\mathbb{R}^{L_n - 4}$, two monitoring statistics can be formed.

$$m_{psd-rg} = \sum_{n=1}^{N} \mathbf{p}_{n_{psd-rg}}^T \mathbf{Q}_{n_{psd-rg}}^{-1} \mathbf{p}_{n_{psd-rg}} \tag{4}$$

$$m_{dplr} = \sum_{n=1}^{N} \mathbf{p}_{n_{dplr}}^T \mathbf{Q}_{n_{dplr}}^{-1} \mathbf{p}_{n_{dplr}} \tag{5}$$

These statistics are derived from the Baseline algorithm [5]. The matrices $\mathbf{Q}_{n_{psd-rg}}$ and $\mathbf{Q}_{n_{dplr}}$ are approximated as:

$$\mathbf{Q}_{n_{psd-rg}} = \mathbf{N}_{n_{psd-rg}}^T \mathbf{R}_{n_{psd-rg}} \mathbf{N}_{n_{psd-rg}} \tag{6}$$

$$\mathbf{Q}_{n_{dplr}} = \mathbf{N}_{n_{dplr}}^T \mathbf{R}_{n_{dplr}} \mathbf{N}_{n_{dplr}} \tag{7}$$

where $\mathbf{R}_{n_{psd-rg}}$ and $\mathbf{R}_{n_{dplr}}$ correspond to the covariance matrix of the sub-vectors of residuals $\mathbf{r}_{psd-rg}$ and $\mathbf{r}_{dplr}$ expressed in the satellite space for receiver n.

$$\mathbf{R}_{n_{psd-rg}} = \mathbb{E}\left[\mathbf{r}_{n_{psd-rg}}\ \mathbf{r}^T_{n_{psd-rg}}\right] \tag{8}$$

$$\mathbf{R}_{n_{dplr}} = \mathbb{E}\left[\mathbf{r}_{n_{dplr}}\ \mathbf{r}^T_{n_{dplr}}\right] \tag{9}$$

Two other statistics can be computed with the concatenated parity vectors $\mathbf{p}_{c_{psd-rg}}$ and $\mathbf{p}_{c_{dplr}}$:

$$\mathbf{p}_c^T = \left[\mathbf{p}_1^T\ \mathbf{p}_2^T\ \cdots\ \mathbf{p}_N^T\right] \tag{10}$$

The statistics are then:

$$m_{c_{psd-rg}} = \mathbf{p}^T_{c_{psd-rg}}\mathbf{Q}^{-1}_{c_{psd-rg}}\mathbf{p}_{c_{psd-rg}} \tag{11}$$

$$m_{c_{dplr}} = \mathbf{p}^T_{c_{dplr}}\mathbf{Q}^{-1}_{c_{dplr}}\mathbf{p}_{c_{dplr}} \tag{12}$$

with the matrix $\mathbf{Q}_c$ corresponding to the covariance of the two concatenated parity sub-vectors $\mathbf{p}_c$. The matrix $\mathbf{Q}_c$ can be constructed in blocks, where each block is the expected value of a pair of measurement sets, m and n. According to [11]:

$$\mathbf{Q}_c[i,j] = \mathbb{E}\left[\mathbf{p}_i\ \mathbf{p}_j^T\right] \tag{13}$$

Following the explanation by [11], if the errors between the residuals are independent, $\mathbf{Q}_c$ can be constructed as a block-diagonal matrix from the covariance $\mathbf{Q}_n$ for each measurement set n, which gives:

$$\mathbf{Q}_c[i,j] = \begin{cases} \mathbf{0} & i \neq j \\ \mathbf{Q}_l & i = j \end{cases} \tag{14}$$

The two methods outlined for forming the CERIM Baseline monitoring statistics (sum or concatenated vector) are equivalent; however, it is essential to note that constructing the covariance matrices correctly is crucial to obtain a good probability distribution of false alarms (PFA). In this study, the covariance matrices for these two CERIM monitoring statistics, pseudo-range and Doppler, are estimated via the methods outlined in [12].
These Baseline monitoring statistics must have an anomaly detection threshold S. An alert is triggered if:

$$m_{psd-rg} > S_{psd-rg} \rightarrow alert \tag{15}$$

$$m_{dplr} > S_{dplr} \rightarrow alert \tag{16}$$

This double CERIM monitoring statistic will theoretically be more robust to inconsistencies, as we will see in section 4.

3. Carrier to noise ratio C/N_0 surveillance

When a GNSS receiver approaches the spoofer, the power of the received signal attempting to spoof increases. The area where this signal is strong can be relatively large. This results in a notable increase in the signal-to-noise ratio (SNR) of receivers located within the spoofer's area of influence because signals from GNSS satellites are generally weak compared to those from the spoofer. To standardize these measurements, the C/N_0 ratio, which corresponds to the signal-to-noise ratio normalized to a 1 Hz frequency, is used. This method allows for the elimination of bandwidth variations between different receivers, making the C/N_0 ratio more consistent within a cooperative receiver network. Consequently, when the spoofer gets closer to a GNSS receiver, the receiver's C/N_0 ratio increases significantly due to the increased signal. Conversely, when a jammer is near a receiver, this C/N_0 ratio decreases significantly due to the increased noise.

The surveillance statistic resulting from this C/N_0 monitoring ([13], [14]) for each receiver is:

$$\alpha(t) = -(\mathbf{c}_t - \boldsymbol{\mu}_t)^T\mathbf{S}_t^{-1}\mathbf{1} \tag{17}$$

with:

- $\mathbf{c}_t$ vector of C/N_0 for all visible satellites l at time t by the receiver:

$$\mathbf{c}_t = \left[\frac{C_{1,t}}{N_0 + J_t}, ..., \frac{C_{l,t}}{N_0 + J_t}\right] \tag{18}$$

- $\boldsymbol{\mu}_t$ vector containing the average C/N_0 associated with each satellite before time t:

$$\boldsymbol{\mu}_t = \begin{bmatrix} \mu_{1,t} \\ \vdots \\ \mu_{l,t} \end{bmatrix} \tag{19}$$

- $\mathbf{S}_t$ covariance matrix of the observation vector $\mathbf{c}$:

$$\mathbf{S}_t = \begin{bmatrix} \sigma^2_{1,t} & 0 & .. & 0 \\ 0 & \sigma^2_{2,t} & .. & 0 \\ .. & .. & .. & .. \\ 0 & 0 & .. & \sigma^2_{l,t} \end{bmatrix} \tag{20}$$

Additionally, the surveillance statistic can be adapted to pool data from multiple receivers:

$$\alpha_{global}(t) = \frac{1}{N} \sum_{n=1}^{N} \alpha_n(t) \tag{21}$$

This yields two surveillance statistics: one can have an individual or collaborative statistic. The most interesting aspect is to observe the behavior of a single receiver to understand its performance when operating in challenging environments (vegetation cover, masking, and multipath).

4. Spoofing test

This section applies theoretical principles to real data to test different surveillance statistics. All experiments are based on real data; however, for obvious safety and legal reasons, spoofing is simulated. The real data are then implemented with more or less logical bias depending on the type of attack, inducing different positions for the receivers.

4.1. Test on the C/N_0 surveillance statistic

Figure 1 presents a test on the percentage of receivers affected by a jamming-type attack. When such an attack impacts a receiver, it is estimated that all satellites observed at time t are affected, resulting in a significant jump in the C/N_0 surveillance statistic.

Figure 1 indicates that when 25% of the receivers experience a 5 dB-Hz drop in the C/N_0 ratio, the attack becomes apparent on the surveillance statistic. According to [15], when the power of the rebroadcast jamming signal exceeds that of the real signal by 4 dB, it can disrupt the authentic signal reception by the target receiver within less than 50 minutes, allowing the receiver to then track the spoofing signal instead. Therefore, it is recommended to implement this type of surveillance for each receiver, although sharing this data is crucial in a collaborative usage to precisely locate affected receivers. The key is to assess the drop in the C/N_0 ratio, for instance under vegetation cover, and take into account these different scenarios to reduce false alarms. The success of these tests will depend on the threshold chosen to maintain a low probability of false alarm rate (PFA). Using data collected over 1 hour by 2 receivers, Figure 2 presents two false alarm probability distributions for the C/N_0 surveillance statistic: one for the fixed receiver and the other for the mobile receiver operating by car in a semi-urban environment over approximately 1 hour.

The analysis of the curve in Figure 2 shows different PFA distributions, allowing for the definition of a robust threshold to differentiate between natural variations and intentional jamming or spoofing

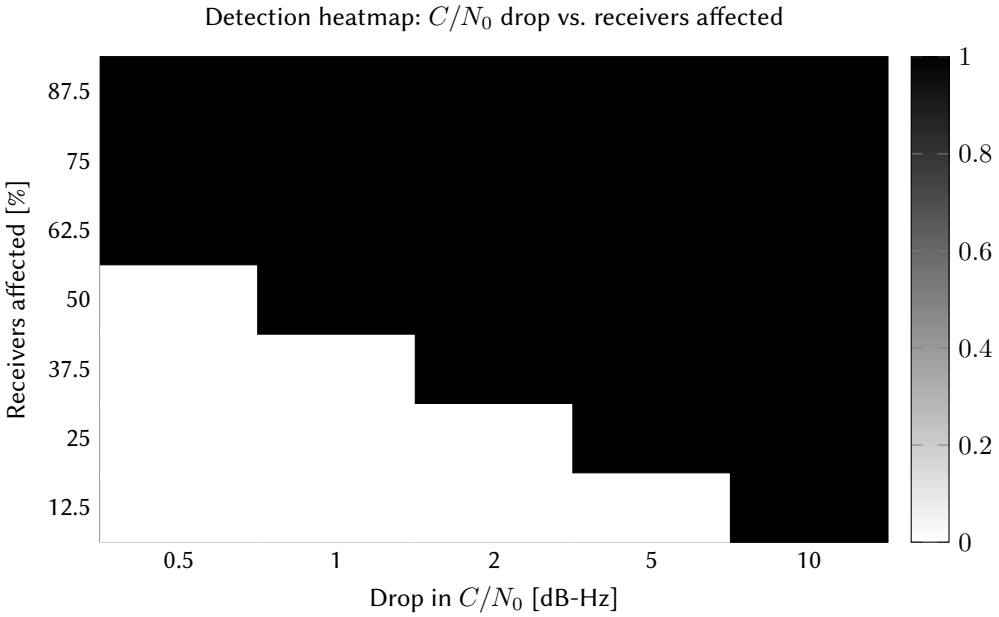

Figure 1: Detection capability depending on C/N_0 drop and proportion of receivers affected. White = no detection; Black = detection.

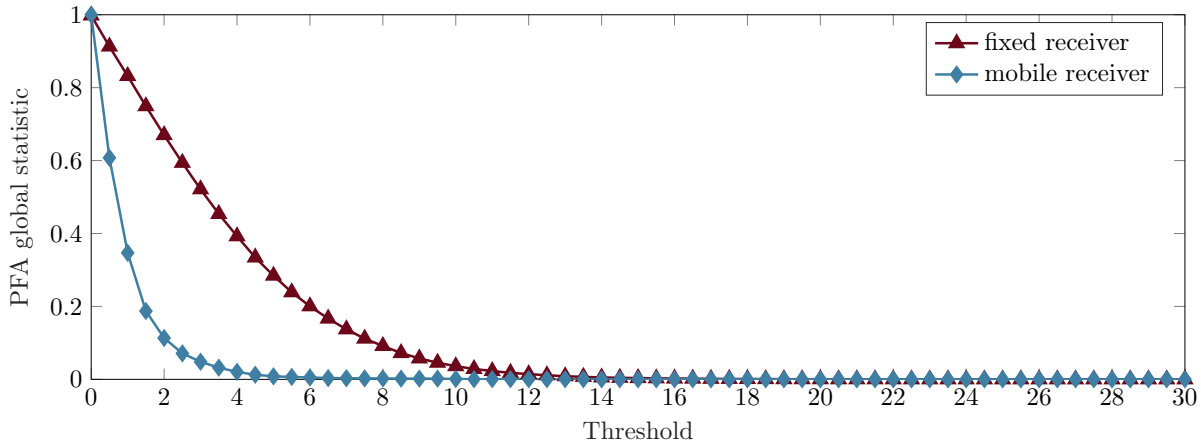

Figure 2: Distribution of PFAs of the global C/N_0 statistic from data acquired by 2 receivers over 1 hour. One receiver was mobile in a semi-urban environment, and the other was fixed during the acquisition period.

attacks. The difference between the distributions can be explained by the fact that, when C/N_0 values are stable, the covariance matrix has low values, making its pseudo-inverse very large. Thus, even small variations in C/N_0 result in significant changes, unlike in an environment with larger variations, where the pseudo-inverse is small and reduce fluctuations. These natural variations affect GNSS signals less significantly than intentional human-induced degradations.

4.2. Evaluation of CERIM against common spoofing attacks: impact of the position repeater

For this test, the 4 receivers will undergo common GNSS spoofing whereby the signals are repeated. The spoofer acts as a GNSS signal repeater: it captures the received signals and then retransmits them after a delay, thus misleading the receiver about its position by positioning it at the location of the spoofer. Implementing this type of spoofing is relatively simple: it involves capturing signals at a given location and sending them back amplified. This creates an area of influence around the spoofer. However, to enhance its effectiveness, the spoofer must precisely adjust the parameters of the spoofed

signal and adapt the spoofing environment to optimize the impact of the spoofing. The difference between a classic repeater and an "all-satellite" repeater lies in the number of satellites the spoofer will spoof: the classic repeater only allows partial spoofing (of a few satellites), whereas the all-satellite repeater enables full spoofing by repeating the signals of all satellites.

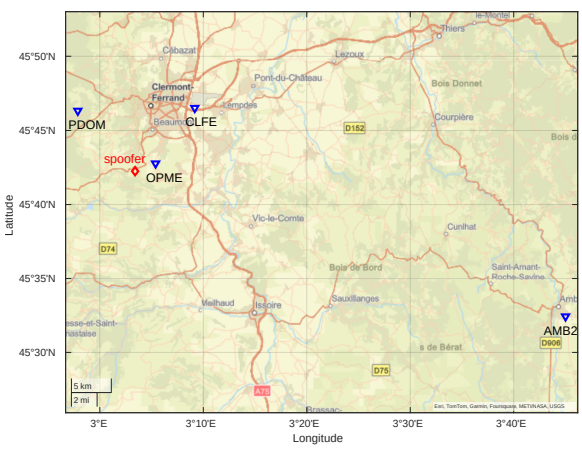

Figure 3: Receiver position and localisation of the simulated spoofer

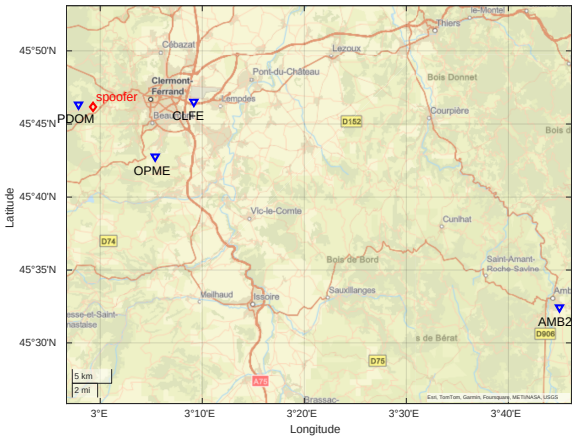

Figure 4: Receiver position and localisation of the simulated sophisticated spoofer

Here, we will simulate a fictitious spoofing by modifying our data to produce a repeater-type spoofing within the network of receivers to be monitored. For this, we will use a fictitious station located 2 km from the OPME receiver. Initially, the spoofer will capture only the satellites visible by the OPME station, which we will refer to as a classic repeater (see figure 3). Here, both our receivers and the spoofer are fixed. The pseudo-ranges and Doppler data are modified accordingly to avoid introducing an additional bias on the receiver's clock bias and clock drift.

This simulation will be repeated k = 500 times, during which a repeater spoofing will be randomly introduced. The duration of this spoofing will be randomly chosen, varying between 50 and 200 seconds, and its start will occur at a random time between t = 500 and t = 3200. Several of these simulations are summarized in Table 1, and they help evaluate the impact of repeater spoofing on the joint CERIM surveillance statistics, including pseudo-ranges and Doppler measurements. The detection threshold is set to achieve a PFA of 10^{-5}.

Table 1
Table summarizing the detection performance for repeater spoofing by the joint CERIM algorithm using pseudo-range and Doppler

Number of spoofed receivers	Repeater Spoofing	
	Classic Repeater	All-satellite Repeater
4/4	49.2%	76.4%
3/4	55.6%	79.8%
2/4	53.2%	79.6%

In Table 1, it's important to note that spoofing attacks that alter all the set of satellites visible to the receiver are much better detected. These attacks are more representative of a receiver behavior in presence of a repeater, since in its normal operation, an individual receiver tends to exclude the unfited satellites with RAIM. In other words, the presence of a mix of signal satellites from the sky and from the spoofer in the navigation solution does not generally last. In fact, the redundancy of information lends weight to inconsistencies detected through the residuals, making it easier to trigger an alarm. The numerous inconsistencies enhance the detection of the attack, highlighting the importance of pooling information to clear any doubt about such attacks. We also observe a decrease in performance with

four spoofed receivers. This anomaly can be explained by the fact that the spoofer's position remains fixed, as does that of the stations. It would be relevant to conduct tests with moving stations, which would allow the surveillance statistic to detect this situation more clearly to remove this uncertainty, as the Doppler would not be consistent in such a scenario.

4.3. Evaluation of CERIM against advanced spoofing attacks: impact on position deviation

The same dataset as in the previous test is used, but this time we will introduce a bias in the data to gradually and significantly modify the position of one of the network's receivers. This manipulation will consistently affect only one of the four receivers. We modified the position of the spoofer, as show in Figure 4. To strengthen the hypotheses, this simulation will be repeated k = 500 times, during which a sophisticated spoofing will be introduced. The duration of this spoofing will be randomly chosen, varying between 50 and 200 seconds, and its start will be set at a random time between t = 500 and t = 3200. This spoofing will generate a consistent position for the targeted receiver, but this position will be inconsistent with the other receivers. The results of the different simulations are summarized in Table 2. The detection threshold is adjusted to achieve a PFA of 10^{-5}. The results obtained in Table 2 are quite similar to those presented in Table 1. However, it is noticed here that the number of detections is higher than that observed during repeater spoofing. This difference is explained by the fact that, in this case, the receiver is artificially set in motion by the spoofer by slowly displacing its position, which makes the Doppler effect indispensable for evaluating the validity of the receivers' PVT (Position, Velocity, Time) estimates. This results in a higher probability of alarm because the residues related to the Doppler effect are more sensitive to inconsistencies. In both spoofing test scenarios, it appears that performance does not substantially depend on the number of compromised receivers. Excellent detections are observed when 50% of the receivers are affected by a spoofing attack.

Table 2
Table summarizing the detection performance for sophisticated spoofing by the joint CERIM algorithm using pseudo-range and Doppler

Number of spoofed receivers	Sophisticated Spoofing	
	Classic Drift	All-satellite Drift
4/4	51.8%	80%
3/4	60.6%	83.2%
2/4	54.2%	84.6%

Different scenarios can be tested: the network can be tightened (receivers close to each other) or spread out (receivers far from each other). Here, we decided to hybridize both approaches to evaluate the impact of the distance between the receivers. However, according to [12], the impact of the distance between the receivers is minimal for CERIM-type methods, provided they can detect the same threat. Indeed, if the receivers are close enough (less than 1 km), the spoofing will also affect them, and they will be deviated from their real positions, causing a jump in their residuals. Conversely, if the receivers are far enough apart (more than 10 km) and if the spoofer seeks to remain discreet, the receivers will not be able to perceive the difference, as they will not catch the spoofed GNSS signal. The attack will go unnoticed by the receiver network. To perceive the differences, one can establish a monitoring statistic on the clock drift, as it changes even in the case of sophisticated spoofing [1].

4.4. Overall Evaluation with Multi-criteria Monitoring on an Advanced Spoofing Attack

By analyzing the performance of each criterion individually, it appears that the theoretical combination of these three criteria allows for very effective detection of the various attacks that compromise GNSS. Thus, one could establish a global and resilient multi-criteria monitoring statistic. However, this hypothesis needs to be confirmed experimentally. To do so, we will again use the same dataset from the four receivers illustrated in Figure 3, and we will adapt the scenario of the intelligent spoofer attack. In this scenario, the spoofer must cause the target receiver to drop by performing a drag-off. This drag-off concept, documented by [7], is crucial for the receiver to eventually lock onto the spoofer's signal rather than the real constellation's signal. The evaluation consists of two successive phases. During the first phase, jamming is simulated with a random decrease in signal power, varying between 5 and 9 dB-Hz for each satellite captured by the receivers. Then, a second phase of spoofing is applied, where the signal gain is randomly increased between 1 and 4 dB-Hz. In this scenario, **detections achieve a rate of 100%** when all receivers are affected, and **98%** when only 50% of them are, with a detection threshold adjusted to achieve a PFA of 10^{-7}. This demonstrates the potential of a multi-criteria approach to enhance the resilience and reliability of GNSS attack detection systems.

5. Discussion

Each criterion covers a specific variable useful for the GNSS receiver, which gives a significant advantage to this multi-criteria approach for anomaly detection. However, it is important to highlight the theoretical nature of the attack: certain biases related to the simulation can lead to degraded performance, even if the tests are conducted under conditions as realistic as possible. Also, the real data used for the various tests come from high-quality receivers (TRIMBLE: NetR9, SPECTRA: SP90M), which provide very stable data with very few errors. The performance of each monitoring statistic provides us with a detailed understanding of their behavior in the event of spoofing attacks. However, it is difficult to define scenarios that are favorable or unfavorable for attack detection. An attack will be more noticeable if all receivers detect the same threat, as it will not appear coherent to each of them. A sophisticated spoofing attack that synchronizes its attacks individually on each receiver is highly complex to implement. Indeed, the same spoofer should find a way to attack individually each of the receivers with a specific attack. Added, for the spoofer, to the necessary simultaneous knowledge of the positions of all the receivers, it appears to be something that is far from easy to carry out. Moreover, it is important to underline that this multi-criteria approach would allow for the detection of advanced spoofing cases because, in practice, a spoofer is never perfect. This method incorporates all the variables used by the receiver to localize itself. Thus, it offers robustness against most attacks, as the combination of information can reveal inconsistencies that would go unnoticed if analyzed in isolation.

6. Conclusion

The performance of this multi-criteria solution has shown very promising results, allowing the detection of spoofing attacks on a network of GNSS receivers without much difficulty. However, additional tests are necessary to confirm these performances by varying the spoofing approaches to verify whether the conditions are applicable to other configurations and a different number of receivers. The full experimental validation of this solution remains to be carried out to confirm the expected theoretical and practical benefits. In the long term, this approach seems extremely promising for improving and reinforcing the detection of these attacks.

References

[1] V. Truong, A. Vervisch-Picois, J. Rubio Hernan, N. Samama, Characterization of the ability of low-cost gnss receiver to detect spoofing using clock bias, Sensors 23 (2023) 2735.

[2] E. Axell, E. G. Larsson, D. Persson, Gnss spoofing detection using multiple mobile cots receivers, in: 2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), IEEE, 2015, pp. 3192–3196.

[3] F. Wang, H. Li, Y. Yang, M. Lu, Gnss spoofing detection based on collaborative raim, in: Proceedings of the 2016 International Technical Meeting of The Institute of Navigation, 2016, pp. 748–755.

[4] J. Rife, Collaboration-enhanced receiver integrity monitoring (cerim), in: 2011 14th International IEEE Conference on Intelligent Transportation Systems (ITSC), IEEE, 2011, pp. 13–18.

[5] J. Rife, Collaboration-enhanced receiver integrity monitoring with common residual estimation, in: Proceedings of the 2012 IEEE/ION Position, Location and Navigation Symposium, IEEE, 2012, pp. 1042–1053.

[6] R. G. Brown, Receiver autonomous integrity monitoring, in: Global Positioning System: Theory and Applications, volume 2, American Institute of Aeronautics and Astronautics, 1996, pp. 143–165.

[7] M. L. Psiaki, T. E. Humphreys, Gnss spoofing and detection, Proceedings of the IEEE 104 (2016) 1258–1270.

[8] E. D. Kaplan, C. Hegarty, Understanding GPS/GNSS: principles and applications, Artech house, 2017.

[9] Z. Wu, Y. Zhang, Y. Yang, C. Liang, R. Liu, Spoofing and anti-spoofing technologies of global navigation satellite system: A survey, IEEE Access 8 (2020) 165444–165496.

[10] R. J. Patton, J. Chen, A review of parity space approaches to fault diagnosis, IFAC Proceedings Volumes 24 (1991) 65–81.

[11] L. Yang, J. Rife, Estimating covariance models for collaborative integrity monitoring, in: Proceedings of the 29th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2016), 2016, pp. 1103–1113.

[12] V. Vince, D. Heurguier, A. Vervisch-Picois, J. M. R. Hernan, Optimizing covariance estimation model for collaborative integrity monitoring in heterogeneous receiver satellite environments, in: Proceedings of the 37th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2024), 2024, pp. 3691–3704.

[13] S. Jada, J. Bowman, M. Psiaki, S. Langel, M. Joerger, Identifying car key fobs as a cause of interference at gnss frequencies, in: Proceedings of the 36th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2023), 2023, pp. 4110–4120.

[14] S. Jada, J. Bowman, M. Psiaki, C. Fan, M. Joerger, Time-frequency analysis of gnss jamming events detected on us highways, in: Proceedings of the 35th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2022), 2022, pp. 933–946.

[15] L. HUANG, Z.-c. LV, F.-x. WANG, Spoofing pattern research on gnss receivers, Journal of Astronautics 33 (2012) 884.