Using of Collective Detection for GNSS Signals Authentication

N.Bouny, F Faurie, *M3Systems*
T.Junique, T.Robert, *CNES*
bouny@m3systems.eu, faurie@m3systems.eu
thomas.junique@cnes.fr, thierry.robert@cnes.fr

BIOGRAPHIES

Nicolas Bouny graduated as signal processing engineer from ENSEIRB-MATMECA, Bordeaux, France, and has worked in the fields of GNSS and space systems engineering since 2010. He has worked for M3 Systems company in collaboration with CNES, the french space agency, on many subjects linked to GNSS as constellation simulation, performances analysis, interferences detection and authentication.

Frederic Faurie received the Ph.D. degree from the University Bordeaux 1. He has worked for M3 Systems on many subjects such as multi-sensor hybridization algorithms, precise posistioning (RTK and PPP), fault detection and exclusion and integrity monitoring, performance evaluation, etc.

Since March 2012, Thomas Junique has been working as a radio-navigation engineer in Signals and Equipment Radio-navigation/radio-localization department of the CNES. He works on research and development on spatial GNSS receivers. Moreover, he is responsible of the navigation laboratory in CNES and also manages activities concerning terrestrial receivers (algorithms); especially in integrity field. Prior to joining the CNES, he worked 2 years in a private company, M3 Systems, carrying out some research activities in the CNES navigation laboratory. He graduated from "Ecole Nationale de l'Aviation Civile" ENAC, in Toulouse (FRANCE) in 2009.

Thierry Robert received the Ph.D. degree from the National Polytechnic Institute of Toulouse in 1996. He is currently head of the location/navigation signal and time frequency department in CNES, the French Space Agency. The department's activities cover signal design and processing, receivers and payloads involving location, and navigation systems including GNSS (Galileo, GNSS space receivers), search and rescue by satellite (Cospas-Sarsat, MEOSAR), and Argos. Other activities covered by the department is the time and frequency reference generation including the UTC(CNES) generation.

ABSTRACT

Today, authentication of GNSS signals is a requirement for many applications. The goal is to certify that the received data are the one sent by the GNSS satellites and that no spoofing attack is in progress. That is why new GNSS signals and services, as Galileo Commercial Service, intend to be more robust thanks to the encryption of the spreading code and of the navigation message. In this paper, we propose a new authentication algorithm based on an innovative method for acquisition and PVT computation: the collective detection, in which satellites are acquired collectively rather than sequentially. Moreover, our proposed solution relies on a deported architecture where a processing centre located on a base station provides authentication services to every GNSS receivers in the neighbourhood.

1 INTRODUCTION

In a context of growing development of critical GNSS applications and services, the ability of a GNSS receiver to guarantee the authentication of received signals, and to detect spoofing attempt, will become mandatory for a lot of use cases.
The goals of every GNSS authentication algorithms are to ensure that, on the one hand, the received navigation message is the one emitted by each satellite and that, on the other hand, the computed pseudo-ranges are correct. Three main strategies are described in [12] to disturb GNSS signals:

- Meaconing strategy, which consists in delaying GNSS signals without modify them
- Nulling strategy, which consists in cancelling real GNSS signals and replacing them by synthetic fake signals
- Non-coherent superposition strategy, which consists in adding synthetic fake signals to real ones.

The quality of an authentication technique can be evaluated thanks to several criteria like the accuracy of the authenticated position, the response time, the probability of false alarm or the ability of the algorithm to detect several type of spoofing.

A lot of authentication methods have been developed and studied over the past few years. In [4] and [5], the authentication is made by controlling the power of the received signal thanks to the AGC (Automatic Gain Control) level. Indeed, a spoofer is often characterised by a high power level. However, multipath can raise false alarm with these methods.
Cryptography is also widely used for GNSS authentication purpose. In particular, Galileo will use these techniques in its new signals for commercial service [6]. The encryption can be applied on the spreading code or on the navigation message. This latter can be symmetric, i.e. the same key is used to encode and decode the message, or asymmetric, i.e. a public key is used to encrypt the message and a private key is used to decrypt the message. Some methods of navigation message encryption are described in [7], [8] and [9]. These technics are very robust but suffer from a long authentication time. Moreover, encryption cannot detect attack of meaconing type.
Less complex technics based on navigation message and raw measurements coherence control can also protect receiver from some attacks [10]. It consists in verifying that the evolution of satellites orbits, satellites clocks, C/No measurements and Doppler measurements are not disturbed. A comparison of received ephemeris and almanac with those received in an encrypted message allows also to detect some issues.

The contribution of this paper consists of an innovative GNSS signals authentication algorithm based on collective detection method. The collective detection is an acquisition method that allows using more efficiently multiple GNSS signals in challenging environments. It follows a vector approach as strong signals are acquired collaboratively to assist the detection of the weaker ones.
The objective of the algorithm presented in this paper is to apply the collective approach to detect and identify one or several spoofers added on real GNSS signals. We propose a remote GNSS authentication solution, where the algorithm is implemented on a secure base station called "authentication centre" that receives measured pseudoranges from the GNSS rover terminal. The detection is performed by evaluating degradation and dispersion of the PVT computed by the collective detection method.
To analyse the efficiency of this method, different cases of spoofing have been considered: non coherent superposition, meaconing or corruption of the navigation message. However, all these cases can be simulated by a bias added on the pseudo-range.
This paper is structured as follows. Section 2 gives an overview of the collective detection for positioning computation in general. Then, section 3 explains how this method is used for GNSS signals authentication. The results of the simulation tests that shows the efficiency of this method are given in section 4 before a conclusion in section 5.

2 COLLECTIVE DETECTION THEORY

2.1 Algorithm description

The Collective Detection method is an acquisition technique for weak GNSS signals, which has been well described in [1], [2] and [3].
The main idea behind this method is to acquire all signals of a given GNSS constellation collectively rather than sequentially. Therefore, stronger signals make the detection of weak signals easier. The code/phase research for all visible satellites is mapped into a position/clock bias grid to treat all signals collectively.

For each satellite and for each point of this grid, the corresponding pseudo range is differentially estimated with the measurements received by a base station, using the equation below. This equation gives the difference $\Delta\rho_k$ between the estimated pseudo-range at the base station and the measured pseudo-range at the receiver for satellite k.

$$\begin{aligned}\Delta\rho_k = &-\cos(az_k)\cos(el_k)\Delta N - \sin(az_k)\cos(el_k)\Delta E \\ &+ \sin(el_k)\Delta D + c.\Delta B\end{aligned} \quad (1)$$

Where:

- az_k and el_k are respectively the elevation and the azimuth of satellite k
- ΔN, ΔE, ΔD correspond to the difference between the receiver position and the base station position in the NED coordinates frame
- ΔB represents the pseudorange variation due to clock bias between the receiver and the base station
- c is the speed of light

Then, an estimation of the code delay ζ_k is deduced thanks to the equation given below.

$$\zeta k = \frac{\left|\rho_{BS,k} + \Delta\rho_k\left(\Delta N_i, \Delta E_j, \Delta D, \Delta B_n\right)\right|_{c.T_{code}}}{c.T_{code}}.N_{code} \quad (2)$$

T_{code} is the code period, N_{code} is the number of chips per period and [.] represents the modulo operation. This estimation of the code delay is used to build a local replica of the signal, which is correlated with the received signal to obtain the individual detection metric of the satellite k as follows.

$$D_{individual} = \left|S(\varsigma_k)\right|^2 \quad (3)$$

S(.) represents the correlation operation. The Doppler frequency shift must be estimated and compensated in the received signal before the correlation.
Then, the collective detection metric is the sum of the individual detection metrics of each satellite.

$$D_{individual}\left(\Delta N_i, \Delta E_j, \Delta D, \Delta B_n\right) = \sum_k D_{individual}(\varsigma_k) \quad (4)$$

Finally, a single metric is associated with each parameter quadruplet $(\Delta N_i, \Delta E_j, \Delta D, \Delta B_n)$. The highest metric value gives the combination of parameters $\Delta N_i, \Delta E_j, \Delta D$ and ΔB_n that correspond to the likeliest receiver position.

2.2 Required inputs and implementation strategy

In order to compute a PVT solution using this algorithm, the following data are required:

- Satellites ephemeris, used to compute their elevation and azimuths used in equation (1). These ephemeris can be read into the navigation message. They are also used to compute satellite velocity and therefore to estimate the Doppler frequency shift
- The base station position
- The pseudorange measurements for all visible satellites at the base station.

It can be noticed that all these inputs can be provided by the base station.

An effective implementation of the collective detection algorithm should follow the steps given below:

1- Establish a spatial and time uncertainty domain for the receiver around the base station and deduce the search grid of the algorithm.
2- For each point of the search grid, apply the collective detection principle described in the previous section.
3- Make an iterative redefinition of the search grid, since the uncertainty is reduced at each execution of the algorithm, in order to have a better resolution.
4- Find the PVT solution thanks to the result of the step 2.

It has to be noticed that the quality of the solutions provided by the collective detection is related to the satellites geometry, to the number of satellites, to the search grid resolution and to the signals power. The expected accuracy is about tens meters. However, the acquisition quality is improved compared to the sequential method.

The main drawback of the collective detection method is the high number of points in the search grid to obtain a sufficient resolution. A compromise has to be found between the resolution and the search grid size. Indeed, a better resolution helps to detect weak signal and improves the precision of the position estimation. However, a higher number of points in the search grid increase the computational burden.

3 COLLECTIVE DETECTION FOR GNSS AUTHENTICATION

3.1 General Overview

Our proposed algorithm takes advantage that the PVT estimation is generally overdetermined from a mathematical point of view. Assuming that the authentic GNSS signal number is sufficient to compute an unspoofed PVT at each epoch, the proposed method relies on multiple PVT estimated from different measurement subsets. In a similar way as RAIM [11], this process ensures that at least one solution is unspoofed.

Based on the approach described in section 2, we propose a remote GNSS authentication solution, where the algorithm is implemented on a secure base station called "authentication centre".

The collective detection used in our authentication solution is based on a correlation between pseudorange measurements instead of a correlation between the received signal and a local replica. Thus, the GNSS rover terminal, which GNSS measurements have to be authenticated, sends its measured pseudoranges and computed PVT p_{rx} (which is not based on a collective method) to the base station.

Then, the authentication algorithm uses the collective detection to compute the PVT solution with all satellites and to compute the PVT solution of selected quadruplet of satellites formed with visible GNSS satellites. The detection of a spoofer is realised analysing the dispersion of these PVT solutions.

Finally, when a problem is detected, the identification of the spoofed satellites is performed by evaluating the degree of involvement of each visible satellite in the degradation of the PVT solution.

The main advantage of this method is that it does not require the RF signal but only raw measurements provided by the receiver.

3.2 System Architecture

The whole system architecture of our authentication solution is shown on the figure below.

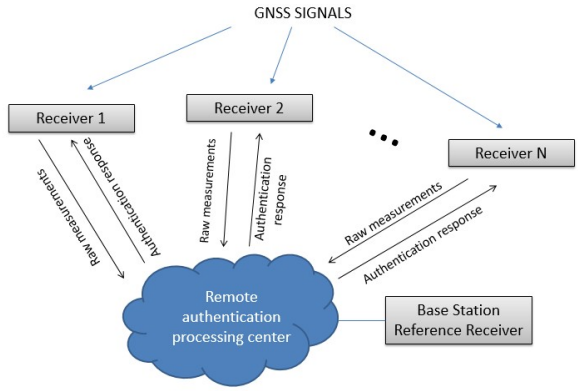

Figure 1 – Illustration of our authentication system architecture

Receivers, which want to authenticate GNSS signals, send their raw measurements to the authentication centre. This latter uses our algorithm based on collective detection to provide a response to receivers. The authentication centre is linked to a receiver capable of processing encrypted signals that provides reference data used during authentication processing.

A deported architecture allows to have less constraints about computational burden and to dispose of a reference receiver compatible with encrypted signals.

Receivers must transmit the following data to the authentication centre:

- The list of visible satellites

- The pseudorange measurements
- The computed PVT solution

The reference receiver must provide the following data to the authentication centre:

- The list of visible satellites
- The pseudorange measurements
- Its computed position
- Satellites ephemeris (or directly satellites position, elevation and azimuth)

The transmission of the receiver data to the base station and the transmission of authentication response from the base station to receivers requires the building of a link communication and should be realised automatically when an authentication is asked.

3.3 Detailed Procedure

The complete procedure of the authentication algorithm can be divided into three parts: the metrics computation, the detection and the identification of the potential spoofer. It has to be noticed that the first one represents the main part of the computational burden. The third one is performed only if an attack has been detected in the second one.

After having received the required data from the receiver to authenticate and from the reference receiver, the processing centre uses the following steps, based on the collective detection, to realise the metric computation part.

1. Definition of the 4D collective detection search grid, around the base station position.
2. For each point of the grid and for each satellite, the "estimated" pseudorange is derived from pseudoranges provided by the reference receiver (see equation 1). The "estimated" code phase is deduced (see equation 2).
3. Simultaneously, the "observed" code phase is deduced from the pseudoranges sent by the receiver.
4. The "estimated" and the "observed" code phases are correlated to give the individual metric of each satellite for each point of the grid (see equation 3).
5. The individual metrics are summed for all satellites (see equation 4). The maximum value of this sum on the grid gives the PVT solution with all satellites, called p_{all}
6. Quadruplets of satellites are formed with all visible satellites. All possible quadruplets are considered. The GDOP (Geometric Dilution of Precision) of each quadruplet is computed. Only quadruplets with a GDOP lower than a predefined threshold called T_{GDOP} are kept for the next steps of the algorithm.
7. For each remaining quadruplets, the step 5 is performed again to compute the estimation of the receiver position provided by the quadruplet *i* and called $p_{quad,i}$

The seven previous steps give all metrics required by the second part of the algorithm to detect a potential spoofing attack. This detection is realised as follows.

1. The dispersion of the positions $p_{quad,i}$ provided by all quadruplets is evaluated through the computation of the standard deviation σ_{p-quad}. This dispersion is assessed in the North/East frame only.
2. The distance d_{Ls-CD} between the position computed by the collective detection p_{all} and the position computed by the receiver p_{rx} is computed. This distance is also assessed in the North/East frame only.
3. A spoofing attack is detected if:

$$3.\sigma_{p-quad} > T_{std} \quad (5)$$

OR

$$d_{Ls-CD} > T_{Ls-CD} \quad (6)$$

T_{std} and T_{Ls-CD} are predefined parameters. In other words, we consider that if the positions given by the quadruplets are very scattered or if the collective detection position estimation is far from the position computed by the receiver, a spoofing attack is in progress.

If an attack is detected, the goal is to identify which satellite(s) causes the issue, in order to indicate to the receiver to reject it. This is the purpose of the third part of the algorithm. This identification is done by evaluating the degree of involvement of each visible satellite in the degradation of the PVT solution, thanks to the following steps.

1. A counter initialised to zero is assigned to each satellite.
2. For each quadruplet i, if the distance between the position $p_{quad,i}$ and the position p_{rx} is higher than $\alpha.\sigma_{p-quad}$, the counter of each satellite of the quadruplet is incremented. Noticed that α is a predefined parameter.
3. The counters of all satellites are normalised to take into account the different occurrence rate of each satellite in the subset due to the GDOP-based subset selection. The satellite with a counter higher than a predefined threshold T_{count} are considered as spoofed.

The use of these counters could allow to detect and to identify a spoofing attack on multiple satellites.

4 RESULTS

4.1 Test environment description

Extended tests have been realised to evaluate the efficiency of our authentication solution. To make the simulations easier, we consider the rover is static.

Four scenarios have been considered. Each scenario differs from each other by the geometry of the simulated GNSS constellation. The sky views of these four constellations are given by the figures below.

Each type of classical spoofing attack can be simulated by a bias added to the pseudorange measurements of the receiver.
The parameters of the algorithm used for the tests are listed in the Table 1. Two cases of detection parameters have been compared. The first case corresponds to low detection bounds and on the contrary, the second case corresponds to higher detection bounds.

We can note that the results of every simulation test have been averaged on fifty iterations.

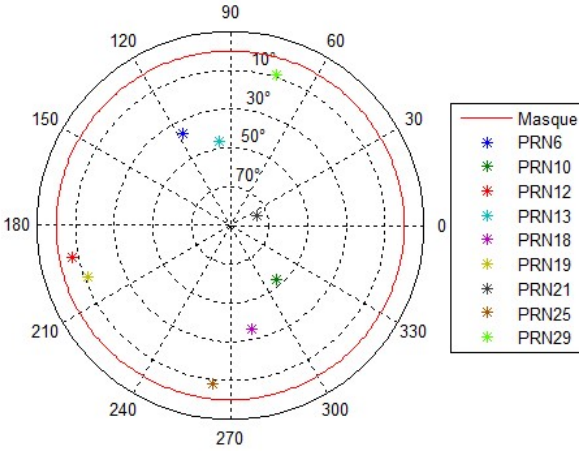

Figure 2 – Constellation geometry of scenario 1

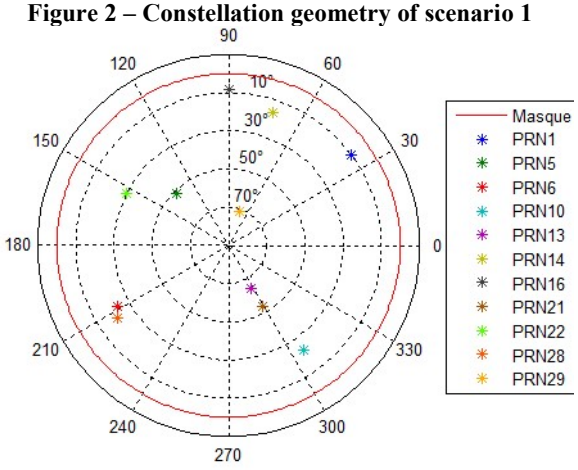

Figure 3 – Constellation geometry of scenario 2

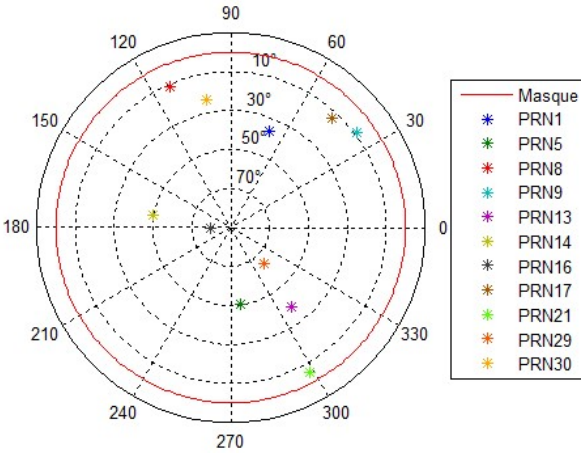

Figure 4 – Constellation geometry of scenario 3

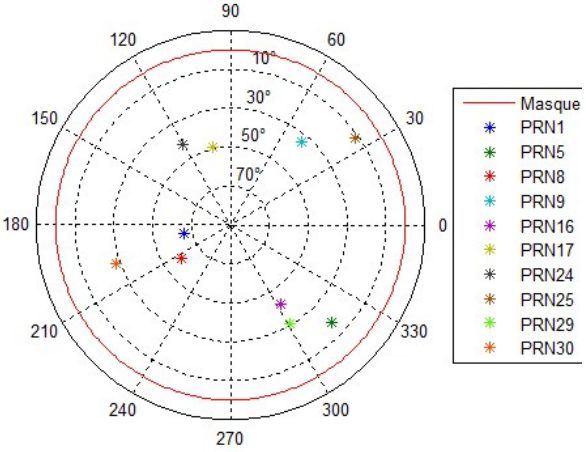

Figure 5 – Constellation geometry of scenario 4

Table 1 – Parameters of the algorithm for the two detection cases studied

Parameter	Description	Value in case 1	Value in case 2
T_{GDOP}	GDOP threshold for satellites quadruplet selection	7	7
T_{std}	Threshold on the dispersion of the position computed by the satellites quadruplets	10m	30m
T_{Ls-CD}	Threshold on the distance between collective detection solution and receiver solution	5m	10m
α	Identification threshold factor	1	1
T_{count}	Threshold for the identification counter	0.5	0.5

4.2 Evaluation of the false alarm probability

The evaluation of the false alarm probability is a crucial point to characterise the efficiency of a detection algorithm. This probability is calculated as the number of

spoofing detection made by the algorithm when there is no spoofer added on scenarios.
Table 2 gives the probability of false alarm obtained with the four scenarios and with the two cases of detection parameters.

Table 2 – False alarm probability for the different tested scenarios

	Case 1	Case 2
Scenario 1	38%	0%
Scenario 2	26%	0%
Scenario 3	38%	0%
Scenario 4	18%	0%

The false alarm probability is null with high detection bounds (case 2). With lower bounds, results depend on the constellation geometry but false probability is not negligible. In 60% of false detection cases, no spoofer is identified among the visible satellites. Consequently, false alarms are not necessarily harmful for the receiver.

4.3 Study of the bias amplitude of the spoofer

In this second series of tests, a spoofed satellite is chosen on each scenario (PRN21 in scenario 1, PRN10 in scenario 2, PRN13 in scenario 3, PRN25 in scenario 4) and several amplitudes of its bias are tested. Figure 6 shows the detection probability obtained in each scenario with the two cases of detection parameters. Figure 7 gives the percentage of cases where the spoofed satellite is correctly identified and the percentage of cases where one or several spoofer are wrongly identified.

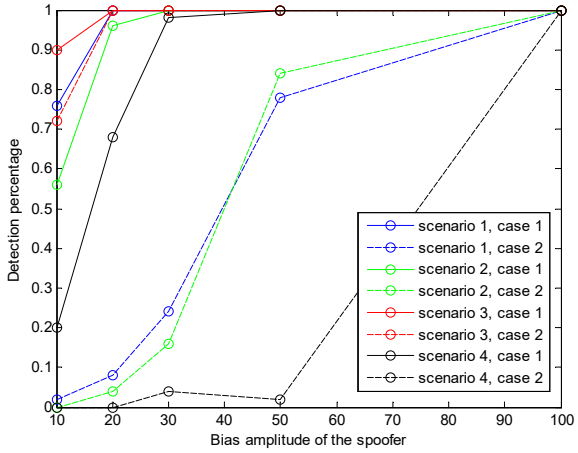

Figure 6 – Detection probability for the four scenarios and the two detection parameter cases

With the case 1 of detection parameters, the spoofing detection probability is always higher than 95% detected when the bias amplitude is greater than 30 meters. In case 2, with higher bounds, the results are more related to the constellation geometry but in all cases the bias amplitude must be higher than 50 meters to have an acceptable detection probability
The percentages of correct identification of the spoofed signal after the detection are close to 100% with a bias higher than 30m. The percentages of wrong detection are weak and acceptable. Note that the two different cases of detection parameters have no impact on identification results.
The non-detection observed for a spoofer with a bias amplitude lower than 30 meters is not necessarily harmful for the receiver since the impact on the PVT computation is possibly low.

4.4 Tests with spoofers at different elevation

In the following tests, we tried to determine if the elevation of the spoofed satellite has an impact on the detection and identification results. To do so, we fix the bias amplitude of the spoofer to 50 meters and we test different spoofed satellite. The obtained detection and identification probability are grouped in Table 3 and Table 4 respectively.

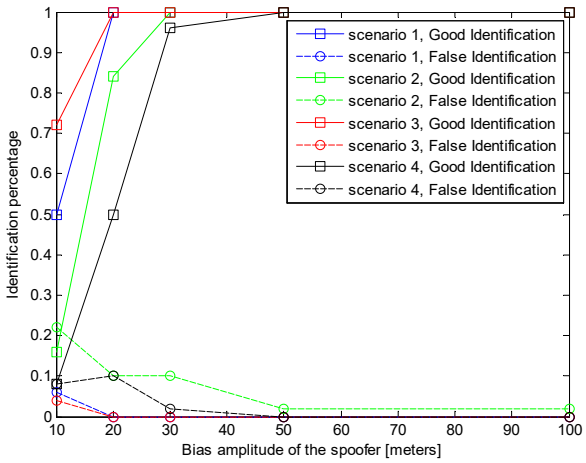

Figure 7 – Percentage of correct and wrong spoofer identification for the four scenarios

Table 3 – Detection probability for spoofers with different elevation

	Spoofed	elevation	Case 1	Case 2
Scenario 1	PRN10	53.4°	100%	100%
	PRN12	6.87°	100%	100%
	PRN13	46.62°	100%	100%
Scenario 2	PRN5	51.33°	100%	100%
	PRN16	8.02°	100%	12%
	PRN29	71.5°	100%	72%
Scenario 3	PRN1	50.1°	100%	100%
	PRN9	9.01°	100%	70%
	PRN21	5.5°	100%	10%
	PRN30	22.94°	100%	100%
Scenario 4	PRN1	65.75°	100%	0%
	PRN17	49.29°	100%	52%
	PRN30	28.06°	100%	86%

Table 4 – Correct and false identification probability for spoofers with different elevation

	Spoofed	elevation	Correct id.	False id.
Scenario 1	PRN10	53.4°	100%	0%
	PRN12	6.87°	100%	0%
	PRN13	46.62°	100%	0%
Scenario 2	PRN5	51.33°	100%	0%

	PRN16	8.02°	100%	0%
	PRN29	71.5°	100%	0%
Scenario 3	PRN1	50.1°	100%	0%
	PRN9	9.01°	100%	0%
	PRN21	5.5°	96%	18%
	PRN30	22.94°	100%	0%
Scenario 4	PRN1	65.75°	100%	2%
	PRN17	49.29°	100%	0%
	PRN30	28.06°	68%	72%

The detection is perfect in every test with parameters of case 1. Some spoofers are not so well detected with parameters of case 2, but it doesn't seem to be especially related to the elevation of the spoofed satellite. In particular, the configuration of the scenario 4 makes spoofer more difficult to detect whatever the chosen satellite.

The identification results are also very sufficient. Only two spoofers are not always identified.

4.5 Tests with multiple spoofers

The last test case consists in observing the performance of our authentication algorithm when several visible satellites are spoofed. Different tests have been created with two or three spoofers.

In every case, the spoofing attack is detected by the algorithm, with the two cases of detection parameters. It is explained by the fact that the computed PVT is more disturbed than with only one spoofer. However, the identification step could be more difficult. Table 5 shows the percentages of test iteration where spoofers are totally identified, where spoofers are partially identified and where false identification is made.

Table 5 – Identification results of tests with multiple spoofers

	Spoofed PRNs	Bias	Total id.	Partial id.	False id.
Scenario 1	PRN10 PRN21	50m 50m	80%	14%	10%
	PRN10 PRN6 PRN12	50m 20m 40m	0%	90%	0%
Scenario 2	PRN10 PRN14	50m 50m	84%	16%	2%
	PRN6 PRN14 PRN29	50m 20m 40m	10%	90%	0%
Scenario 3	PRN13 PRN17	50m 50m	100%	0%	0%
	PRN14 PRN17 PRN1	50m 20m 40m	0%	94%	0%
Scenario 4	PRN25 PRN9	50m 50m	0%	0%	100%
	PRN16 PRN30 PRN17	50m 20m 40m	0.02%	0.92%	0.04%

It can be seen that the results are related to the constellation geometry again. With two equivalent spoofers, the identification is always or often complete in scenario 1, 2 and 3. However the identification is always false in scenario 4.

With three spoofers, the identification is often only partial. That means that only one or two spoofed satellites are correctly identified. Indeed, the spoofed satellite with a bias equal to 20m is almost never identified. In this case, we could imagine an iterative process. In a first time, the stronger spoofer are identified and eliminated on the receiver. Therefore, in the next epoch, the remaining spoofed satellite could be identified

5 CONCLUSION

In this paper, a new GNSS authentication algorithm has been presented. This method is based on an innovative acquisition and PVT computation method, called the collective detection. The goal is to compute the PVT thanks to quadruplets of visible satellite, to compute the dispersion of theses computed positions and to evaluate the degree of involvement of each satellite in the solution degradation in order to detect spoofing attack.

Tests have shown the efficiency of the algorithm in different situation. Two sets of detection parameters have been tested. The choice of those parameters will result in a compromise between the false alarm probability and the detection probability. It is also related to the type of spoofing. A spoofer that adds a low bias on the pseudorange needs lower detection bounds. But it raises the false alarm probability.

This method is more efficient if non-spoofed signals are visible. If all satellites are spoofed, the method may not be able to identify all spoofers. However, this goal could be reached with an iterative process.

In the future, our authentication solution will be confronted to more realistic test conditions. The goal is to build a test bench of the system and to use it to detect spoofer added on real GNSS signals.

REFERENCES

[1] Axelrad, P., and B. Bradley, J. Donna, M. Mitchell, and S. Mohiuddin, "Collective Detection and Direct Positioning using Multiple GNSS Satellites," *NAVIGATION, Journal of The Institute of Navigation*, Vol. 58, No. 4, 2011

[2] Cheong, J., Signal Processing and Collective Detection for Locata Positioning System, PhD thesis, University of New South Wales, 2012

[3] Esteves P., Sahmoudi M., Ries L., "Collective Detection of Multi-GNSS Signals", Inside GNSS, May/June 2014

[4] Akos, D. M., "Who's Afraid of the Spoofer? GPS/GNSS Spoofing Detection via Automatic Gain Control (AGC)," NAVIGATION, Vol. 59, No. 4,Winter 2012, pp. 281–290.

[5] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle,"Pre-despreading authenticity verification for GPS L1 C/A signals," Navigation, vol. 61, no. 1, pp. 1–11, 2014.

[6] I.F. Hernandez et al, Galileo's Commercial Service - Testing GNSS high accuracy and authentication, Inside GNSS, Jan/Fev 2015

[7] O. Pozzobon, State of the art in GNSS authentication and opportunities for system evolutions, ENAC, Nov 2015

[8] Mark L. Psiaki and Todd E. Humphreys, GNSS Spoofing and Detection

[9] I. Hernandez et al, Design Drivers, Solutions and Robustness Assessment of Navigation Message Authentication for the Galileo Open Service, Proceedings of the 27th ITM ION, ION GNSS+ 2014

[10] C. Günther, A survey of spoofing & counter measures, Journal of the ION, v61-3, Automne 2014

[11] R. G. Brown et P. Y. C. Hwang. “GPS failure detection by autonomous means within the cockpit”. Navigation, Vol. 33, No. 4, pp. 335–353, Winter 1986

[12] Mark L. Psiaki, Techniques for Spoofing and for Spoofing Mitigation, ENAC/SIGNAV Navigation & Timing Symposium, Nov. 2015