Influence of GNSS spoofing on drone in automatic flight mode

Vervisch-Picois Alexandre, Samama Nel, Taillandier Loize Thierry, Laboratoire SAMOVAR UMR 5157,
Télécom SudParis, CNRS, Université Paris-Saclay Evry, France
alexandre.vervisch-picois@telecom-sudparis.eu

BIOGRAPHIES

Alexandre Vervisch Picois is an assistant professor of TelecomSud-Paris. He received a Phd in 2010 for his work on GNSS indoor positioning. He has been working since 2004 in the GNSS field, on various projects such as indoor location techniques and multipath mitigation methods. His interest for navigation system of UAV comes from his knowledge of GPS system.

Nel Samama is a professor of Telecom Sud-Paris. He received the diploma of engineer in Mechanics and Electricity from the "Ecole Spéciale des Travaux Publics", Paris, in 1985, the M.Sc. degree in Computer Science from the University of Birmingham, UK, in 1985 and the Ph.D. degree in Electrical Engineering and Computer Science from the University of Paris in 1989. He worked for Thales group from 1989 to 1997 where he designed behavioral modeling for microwave and electronic components stressed by high power microwave radiation. Since 1997 his interest is focus indoor positioning methods in general and GNSS in particular.

Thierry Taillandier-Loize obtained his PhD in 2014 at Université Paris 13, Sorbonne Paris Cité. The main part of his thesis was the realization of an original slow metastable argon beam from a magneto-optical trap which have outstanding features. The same year, he joined the "Electronique et Physique" department at Télécom SudParis as Assistant Professor. From 2016, his field of interrest is about indoor geolocalisation based on GNSS signal at TIPIC group of SAMOVAR.

ABSTRACT

Recent years have seen the proliferation in our skies of flying drones otherwise called UAVs (Unmaned Aerial Vehicle). Their current and potential uses are many: from the military uses to leisure activities through business applications like photography, aerial imaging, spotting, pest extermination (like hornets nest), home delivery, etc.
This was made possible and facilitated by the miniaturization and the reduction of the power consumption of Microelectromechanical Systems (Mems), but also by the dissemination of techniques making the navigation easier. We refer of course to satellites geolocation techniques such as the well-known Global Positioning System (GPS) and Global Navigation Satellites Systems (GNSS), which is its extension to all existing constellations. The growing interest in UAVs is obvious, however, this brings some questionings: are there any limits to what a drone can do? This article aims to put the problematic of the drone linked to the vulnerability of the GPS signal and its consequences. Indeed, one of the characteristics of civilian GNSS signals (therefore free to use) is their very low power. A GNSS receiver is therefore easy to decoy by means of a fake GNSS signal that reproduces the aspect of a real signal but contains fake positioning information. Under these conditions, the GNSS receiver embarked by the drone calculates a position which is not the real position. Consequently, the trajectory of the drone is distorted.

We will see, from a theoretical point of view, what happens when a receiver is submitted to a fake signal and the consequences that this induces to the navigation of the drone. Simulations will support our words and laboratory tests on existing UAV navigation systems will be presented.

Key words: drone, UAV, decoy, spoofing, GPS, GNSS

1 INTRODUCTION

One drone operating modes is to fly automatically, that is to say: set in advance a flight plan to be followed by the drone without any intervention of a pilot. The need for automating the flight of drone is real: several applications, like delivering package, would require such capacity. Putting aside the problem of collisions, there is another limitation. Small sized UAVs (from less than 1 kg to 25 kg) are unlikely to embark complementary navigation systems to GNSS. Concretely, this means that, apart from a visual flight (where the drone is directly visible by the pilot), the only means by which the drone knows its position is a GNSS receiver. This is a great strength, since accuracy of GNSS is sufficient to perform a flight under excellent conditions. However, it could also be a great weakness because the dependency to GNSS is thus considerable.

1.1 Principle of Spoofing

It is well known that one can trick a GPS receiver by broadcasting the equivalent of the signals of a complete constellation from an antenna to the ground [Broumadan & Al 2015]. This is particularly the case for GNSS repeaters to provide coverage in areas where signals are more difficult to receive. It is known that a GNSS receiver which receives the signals coming from an antenna of a repeater will calculate the position of the antenna where the external signal is received [Caratori & al 2003]. The external antenna of the repeater (where it receives the external signals) can also be replaced by a constellation simulator. The receiver receiving the signals will then calculate the point that will have been defined in the simulator [Tippenhauer & Al 2011]. This is true if the signals broadcasted by the repeater are powerful enough to dominate the ones of the real GNSS constellation. The signals emitted by the antenna on the ground (or in the air, but in any case exogenous to the satellite navigation system), then replaces, for the receiver, the ones coming from the satellites. These ones are very weak (power between -120 and -130 dBm) and a signal which is 20 dBs stronger can dominate their effects in the correlators of the receiver.

1.2 Previews Studies on GNSS Spoofing

The problem of GPS spoofing has been known for a long time and its effects on the navigation solution (Position Velocity Time) have been widely studied since the appearance of GPS. The attack of a GPS receiver by a lure signal has been explained and carried out by several research teams which have even defined protocols for a successful attack (in order to counteract this attack) [Larcom & Al 2013]. However, except under very specific conditions, if it is possible to detect that a receiver is being attacked, it is practically impossible to cancel the effects of this attack other than with methods requiring use of direct signal processing [Broumandan & Al 2015]. In [Larcom & Al 2013], we can distinguish several degrees of subtlety in the attack that is partially found in [Kim & Al 2012], which identifies three levels of attack mainly defined by the carried out spoofing system: the simplest is a constellation generator, the intermediate level is a synchronized generator on the real GNSS constellation and the most sophisticated consists of distinct transmitters redefining practically a new constellation. The ability to detect attacks then depends on the complexity of the attacking system.

About drones, [Giray 2013] offers a fairly global view of all that drones in general (including sophisticated military drones) may encounter as a type of "hacking" attack on GPS, but also of their remote control system. It highlights the strong dependence of drones on GPS and thus their vulnerability to interference and attacks, which also distinguishes several levels according to their sophistication, taking the definitions of [Kim & Al 2012]. The whole issue of the vulnerability of GPS for drones is particularly concern since the hijack of a CIA RQ-170 drone by Iran in 2011. Iran is suspected of using a fake GPS signal to crash the drone in question. It is partly to answer this question that a very interesting study was carried out by the team of Doctor Humphrey of the University of Austin in Texas on the subject of the drone decoy [Shepard & Al 2012]. Indeed, with an adequate decoy system, it shows that the trajectory of a standard civilian drone (a Hornet mini UAV here) can be reversed, which actually believes itself to be the opposite of the place where it want to go. We show in this paper that spoofing of civilian drones is actually easier.

1.3 Content of the paper

A first part consists of the presentation of spoofing situation for UAV. The geometrical aspects are discussed here with some theoretical elements. Influence of spoofed signal on GNSS receiver is also discussed.

The second part presents simulations with a few cases and the subsequently expected behaviors of the spoofed drone.

The third part present experimentation that define the required power level and procedure to “take control” of the GNSS receiver of an UAV. Follow applications of the spoofing on a real drone in laboratory and without spreading the signal from an antenna to respect the regulation.

This paper is a summary of the results obtained in the context of a french national research agency (ANR) project whose topic was the less than 25 kg drones detection and neutralization.

2 SPOOFING THE GPS OF DRONES

The easiest way to spoof a drone, as we saw above, is to broadcast a fake GNSS signal to the drone. If this signal dominates the one from the satellites, the direct consequence on the GNSS receiver is the calculation of a new position. This position will be defined by the fake signal, itself determined by the one who wants to spoof the navigation system of the drone. Once the drone believes to be at the place where the “spoofer” wants, its behavior will adapt to this new situation.

2.1 Geometrical considerations

Imagine, for example, that one wants to deviate a drone from its trajectory to make it go in the opposite direction to that which it wants to take. The basic idea consists in broadcasting a fake GNSS signal whose, once received by the drone, the resulting calculation corresponds to a point located exactly at the opposite of its direction of arrival. Figure 1 illustrates such a situation.

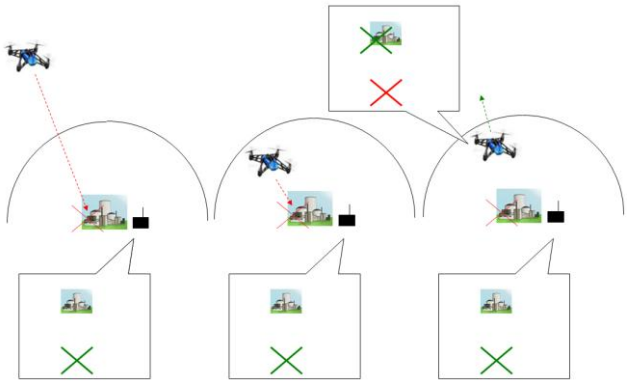

Figure 1 – Expected effect of a full GNSS spoofing

The left side of Figure 1 shows on a drone trying to approach. The half circle represents the area from which the spoofer is active. When entering this area (central illustration), its GNSS receiver is "spoofed". It thus receives a constellation of satellites broadcast by the spoofer causing it to calculate a point that is not the real point (the location of this point is visible on the three illustrations of figure 1). The GNSS receiver of the drone then indicates the coordinates of the "fake point" instead of those of the real position (The coordinates of the "fake point" are obtained by a receiver that is using the signals broadcast by the spoofer to calculate its position). Logically, the drone tries to reach his next waypoint which is no longer in front but behind him. The drone is changing its direction until it comes out of the coverage area of the spoofer (this is illustrated to the right of figure 1). Indeed, in its basic mode of navigation, the drone targets the next waypoint in direct line. If we make believe to the drone that it is located at a sufficiently distant point in the opposite direction from which it comes, it is almost certain that it will turn over because it will believe to be beyond the waypoint that it aims.

2.2 Influence on GNSS receiver

To obtain the previously mentioned behavior, the GNSS receiver of the drone must take the fake signal broadcast by the spoofing device for the real one. There are a number of practical difficulties related to radiation and antenna design that we will not discuss here: the subject of this article is not to develop a system to spoof drones, but to highlight the weaknesses of the today's navigation systems. However, one can wonder about the ability of the GNSS receiver to withstand these attacks and the power levels necessary to take control of them.

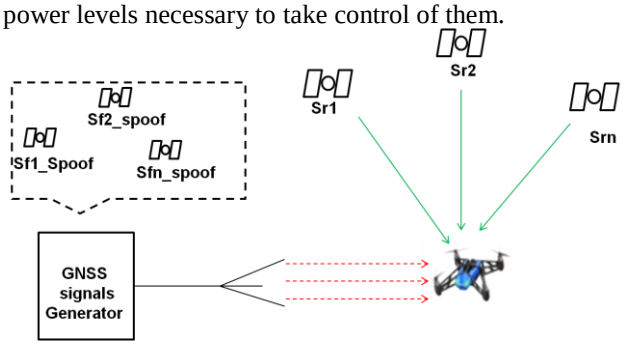

Figure 2 – GNSS spoofing principle

Figure 2 shows the principle of spoofing. The constellation of "Sfx_Spoof" is broadcast in the direction of the drone. This constellation must replace those of the "Srx" for the receiver so that the fake position is calculated. Let us note that it is no obligation that it is exactly the same constellation (the satellites may be different). In order to make this possible, the operating of the receiver must be considered more closely. In normal operation, the receiver calculates the position from the propagation time measurements of the satellites signals and from the positions of the satellites [Kaplan]. The spoofing device artificially creates GNSS signals on which it induces the propagation times corresponding to those they would have if they were actually received from the satellites at a given position (chosen by the spoofer). We note (x_r, y_r, z_r) the coordinates of the true position of the receiver and (x_{sr}, y_{sr}, z_{sr}) those that the spoofer wants the receiver calculates.

$$\rho_1 = \sqrt{(x_r - x_1)^2 + (y_r - y_1)^2 + (z_r - z_1)^2} + cb$$
$$\rho_2 = \sqrt{(x_r - x_2)^2 + (y_r - y_2)^2 + (z_r - z_2)^2} + cb$$
$$\rho_3 = \sqrt{(x_r - x_3)^2 + (y_r - y_3)^2 + (z_r - z_3)^2} + cb$$
$$\rho_4 = \sqrt{(x_r - x_4)^2 + (y_r - y_4)^2 + (z_r - z_4)^2} + cb$$

Figure 3 – Positioning Equations

Let us consider the navigation equation on figure 3. The left part (ρ_i) corresponds to the propagation time measurements for each satellite (in units of distance). x_i, y_i, z_i are the coordinates of the satellites. c is the speed of light and b is the clock bias between the GPS time (or GNSS) and the clock of the receiver. Solving these equations gives the receiver position plus the clock bias. What does happen if the spoofing signals dominate? The equations are the same, but the values change and are now those that the spoofer imposes. However, what is the impact of the propagation time between the spoofer antenna and the one of the receiver? If Δt is this propagation time, then the equations of figure 4 are obtained.

$$\rho_{s1} = \sqrt{(x_{sr} - x_{s1})^2 + (y_{sr} - y_{s1})^2 + (z_{sr} - z_{s1})^2} + c(\Delta t + b_s)$$
$$\rho_{s2} = \sqrt{(x_{sr} - x_{s2})^2 + (y_{sr} - y_{s2})^2 + (z_{sr} - z_{s2})^2} + c(\Delta t + b_s)$$
$$\rho_{s3} = \sqrt{(x_{sr} - x_{s3})^2 + (y_{sr} - y_{s3})^2 + (z_{sr} - z_{s3})^2} + c(\Delta t + b_s)$$
$$\rho_{s4} = \sqrt{(x_{sr} - x_{s4})^2 + (y_{sr} - y_{s4})^2 + (z_{sr} - z_{s4})^2} + c(\Delta t + b_s)$$

Figure 4 – Positioning equations with spoofing

The ρ_{si} are the "spoofed" versions of the measurements of distances, the x_{si}, y_{si}, z_{si} are the positions of the satellites of the decoy system. Similarly b_s is the clock bias between the receiver and the decoy system. Under these conditions, the resolution of the equations of figure 4 gives the position (x_{sr}, y_{sr}, z_{sr}). If this is indeed the case, it is because the Δt linked to the propagation time of the signals between the spoofer and the receiver is common to all the "fake" satellite signals, such as the clock bias. It is therefore exactly the fake position imposed by the spoofer that will be calculated and used by the navigation system of the drone.

It is on these assumptions that the simulations of the following section have been performed.

3 SIMULATIONS

We present here some computer simulations which highlight the behavior of a drone in automatic flight whose GNSS receiver is in the presence of a decoy of the previously described type. This receiver calculates a point from simulated data adapted to the situation, hence

according to the relative position of the drone and the satellites which are supposed to fly above it.

3.1 Description of the simulator

Its organization can be divided into three main functions:

GNSS receiver

The GNSS receiver calculates the coordinates of the point, as a real receiver would do. These coordinates are calculated from the simulated measurements which depend either on the position of the drone, or on the spoofer if the drone is located in the zone of emission of the spoofing signals.

Calculation of the « real » trajectory

This function makes it possible to calculate the true point on which the drone is located, whether it is under the spoofer influence or not. The position from one point to the next is calculated from the displacement vector obtained at the output of the navigation function.

Navigation function

This function uses the output from the GPS receiver to determine the displacement vector it will apply to the drone. In practice this corresponds to the possible changes in direction and engine speed of the drone. The drone decides what it does, based on its current GPS position and the next waypoint to reach. The navigation system considers that a waypoint is reached when the GPS position indicates a point within 3 meters of the waypoint. To simulate a real drone navigation system, the altitude taken into account is the true altitude of the point and not the altitude calculated by the GPS receiver. In a true drone, the altitude is measured by a barometer and / or a sonar, so independently of the GPS.

It is important to note that this simulator focuses on the behavior of the drone in response to a calculated GPS point. It does not enter very deeply into the GPS receiver operation. It considers the outputs of the correlators (therefore the distances measurements) and the ephemerides of the satellites (thus the navigation message) as input data. The antenna effects, digitization, ionosphere effect or other physical phenomena that may influence the quality of the measurements are not simulated. The disturbances are modeled by a Gaussian white noise to which amplitude between 1 and 5 meters is given for each measured distances. This is rather pessimistic for a flight in clear zone. In each case, the measured distances are considered to be "as they should be" if everything is going well for the receiver, being under spoofer influence or not.

3.2 Simulations for some significant cases

For any simulations, a situation is chosen where a drone wishes to point to a waypoint and receives a spoofing signal when it enters a precise zone. It ceases to be under the spoofer influence when it moves away sufficiently (this second zone is wider than the first, illustrating that once the receiver is in tracking mode, the power thresholds for losing the track are lower that for acquisition [Kaplan]). Figure 5 illustrates this operation.

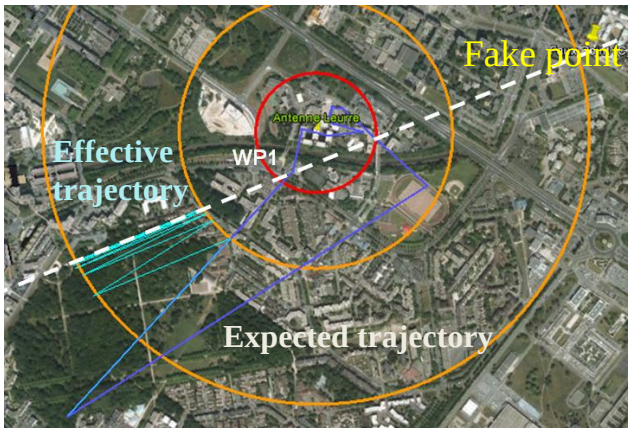

Figure 5 – Spoofing GNSS with opposite fake point

The trajectory constituted of straight lines (in blue) corresponds to the trajectory that the drone wants to make. The area delimited by the second orange circle corresponds to the area where the spoofer is activated. The area delimited by the third circle (orange) delimits the zone beyond which the spoofer no longer acts. The trajectory actually followed by the drone is visible in figure 5. It is interesting to notice that the trajectory of the drone ends up aligning geometrically on the straight line defined by WP1 - Fake point (dashed white line on the line figure).

Another example can be seen in figures 6 and 7, which illustrates the influence of the "distance" of the fake point.

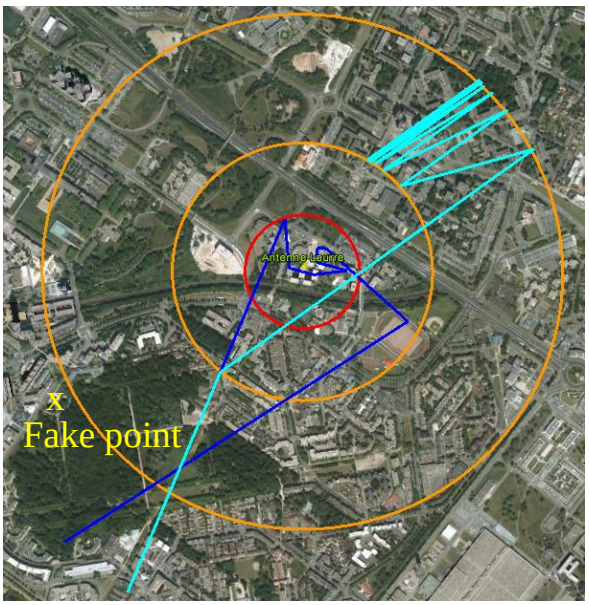

Figure 6 – Spoofing GNSS with near fake point

By comparing figures 6 and 7, it can be noticed that a fake point taken further tends to twist the trajectory more easily. It seems that spoofing is more effective if the fake point is farther from the target waypoint.

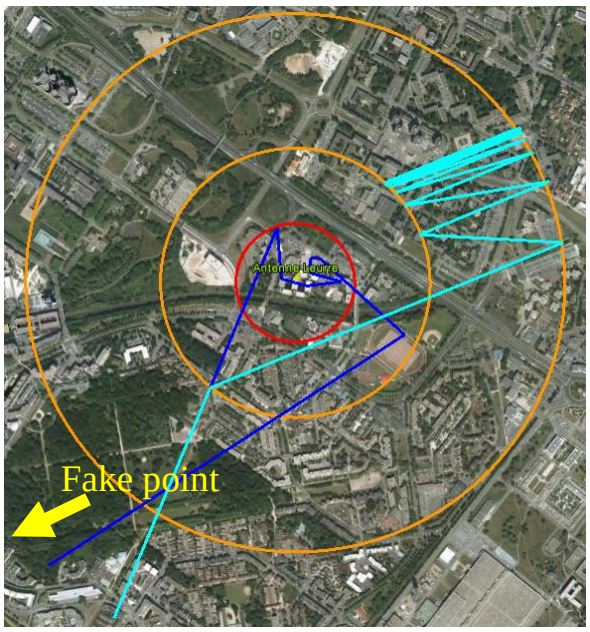

Figure 7 – Spoofing GNSS with far fake point

To make the simulations more relevant, we added a Kalman filter on the receiver position calculation. In this simulation, the instant velocity is supposed to be known (could be delivered by an IMU sensor for example). This velocity is used by the Kalman filter to predict the next state. The setting of the filter is such that the predicition is worthy trusted compared the raw measurements. This results is presented in figure 8.

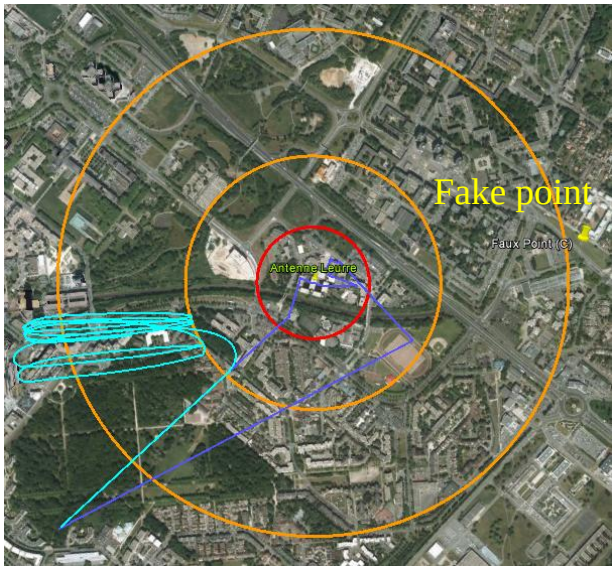

Figure 8 – Spoofing GNSS with kalman filter

It can be seen that the receiver takes a certain amount of time to trust the sudden change in the measurements linked to the spoofer influence. The trajectory is thus more "rounded" than in previous simulations, because of the inertia of the filter (linked to good confidence in the prediction). However, the measurements from the spoofer remain stronger and the alignment previously observed between the trajectory, the waypoint and the fake point is nevertheless occurring.

We are now going to focus on practical realization.

4 EXPERIMENTS

In order to obtain the geometric effects that the simulations have just shown us, it is essential that the decoy signal dominates the signal coming from the constellation. We are trying to determine, for a typical GNSS receiver, under what conditions this is possible.

4.1 Resistance to spoofing of a GPS receiver

We will see the result of various tests that have been performed on a µblox GPS receiver (u-blox 6 Eva 6-T chipset). Some preliminary details must be claryfied:

A GPS receiver has two operating modes:

- Acquisition
- Tracking

The receiver in acquisition mode is searching for the satellites to calculate its position. It is rather unlikely that a drone approaching a site is in this mode, at least not for all the satellites of the constellation. Indeed, if the drone is traveling toward a waypoint, this means that it has a position, thus that it has enough satellites in tracking mode to calculate a position. It is however in this mode that it is most vulnerable to the spoofing signal.
The tracking mode occurs after the acquisition mode. The satellites signals are processed and the receiver calculates its point. The tracking loops of the receiver channels are locked onto the signals from the satellites. It is in this mode that the receiver is operating for most satellites when the drone flies in automatic flight.
What focuses our interest is to know from what value of the power difference between the spoofing signals and the satellite signals the decoy becomes dominant and forces the receiver to compute the point it wants. The relative Power between those signals will thus be our main criterion of evaluation. However, several parameters related to the spoofing signal can be used to define the behavior of the GPS receiver. We chose three from a long list:

- The date, time, and time associated with the spoofing signals compared to “real” signals.
- The relative position of the fake point and the true point.
- The constellation of satellites, identical or different from that of the “real” constellation.

We will see in this experimental part for both acquisition and tracking modes, the influence of different types of spoofing signals (considering the previously defined parameters). This will define which types of signals the receiver will be most vulnerable to.

4.2 Experiments

To evaluate the power difference, we carried out the following experimental set-up:

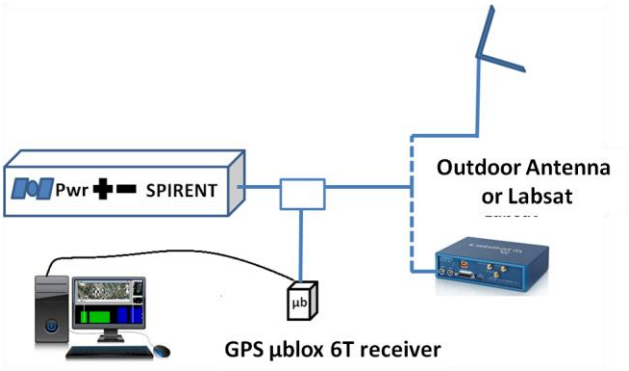

Figure 9 – Testing set for GPS spoofing

For the spoofing signal, a signal coming from a SPIRENT GSS6700 signal generator will be used. For the "real" signal (from the satellites), we used either an external signal brought by an antenna on the roof of the building, or a signal replayed by a LABSAT 2 device, recorded from the GSS6700 signal generator. The advantage of this set-up is to have a fully repeatable scenario with the possibility to have the same constellation for spoofer and "real" signal.

The assembly of figure 9 is used with the Labsat. To ensure that the constellation is exactly the same, the GPS signal at the output of the SPIRENT has been previously recorded in the Labsat: for a given point, at a given date and time. This signal will be considered as the reference signal. This corresponds to the signal of the real constellation "CS". At the output of the SPIRENT, which is transmitting in parallel in exactly the same way as the scenario in figure 1, there is a signal **at the same date and at the same time**, including **the same satellites as CS signal**, but for a point (the "fake point") located at about 300 meters from the first point (this of the Labsat record). The results obtained are presented in the following tables:

Table 1 – Spoofing in Tracking mode

Tracking										
CS/SS (dB)	6	0	-5	-10	-15	-20	-25	-26	-27	-28
Noise increase (dB)	<1	<1	<1	1	3	6	10	Y -11	Y -13	Y

Table 2 – Spoofing in Acquisition mode

Acquisition								
CS/SS (dB)	10	6	0	-5	-6	-8	-10	-15
Acquisition on Spoofing Signal Y/N	N	N	N	N	N	Y	Y	Y

CS/SS is the power ratio between the signal of the constellation CS and the signal of the spoofer SS. When marked "Y", this means that the decoy signal has finally dominated the signal of the constellation sufficiently so that the coordinates of the point computed by the receiver correspond to those of the fake point. A mark "N" means that the receiver still uses the signal of the constellation in spite of the presence of the spoofing signal (the spoofer has no more effect than increasing the noise reception).
In the tracking mode, it is clear that a power difference of at least 26 dB is required in order for the receiver to unlock from the "real" point.
For acquisition, the receiver restarts as after a prolonged loss of signal, so it naturally chooses the strongest signal, however provided that it is strong enough. For a ratio CS/SS between 6 and -8 dB, we are in an intermediate situation where the spoofing signals and the satellite signals have about the same power, so anything can happen. It has been observed, however, that up to -8 dB, the receiver has a preference for real signals, even if they are disturbed. In fact, in the latter situation, the point is calculated with a mixt of the two signals, some real and some from the spoofer, but when the receiver calculates its position, it tends to favor the real signal, probably because it is more consistent with the integrity algorithms of the receiver. This is a possible explanation but without any certainty. One thing is certain that for a ratio CS / SS <-8 dB, the receiver prefers the decoy without any ambiguity.

Let us now see what happens if we use an entirely different constellation, on the same day at a different time.

The signals of the satellites are unchanged, the position of the fake point also. What changes here are the satellites. It is placed in the configuration of the sky **5 hours after that of the satellite signals** (it is recalled that with a constellation simulator, all configurations are possible). The satellites are all different. As a result, we observed that the power levels required for acquisition phase are unchanged. However the tracking presents results very different from those of the first experiment:

Table 3 – Spoofing in Tracking mode with different Constellation

CS/SS (dB)					
Noise increase (dB)	-6	-8	-10	-15	-20
CS/SS (dB)	<1dB +N	Y (slow 30s)	Y	Y	Y

It is observed that this time there is no need to have a power difference of -26 dB so that the receiver prefers the spoofer: -10 dB are enought. At -8 dB the spoofer is finally prefered, but is rather slow because the receiver hesitates between two positions. Concretely, the receiver is looking for satellites permanently. It should also be noted that there is no particularly noticeable increase in noise, which can be understood since the signals are at comparable levels: we see what we already had seen in Table 1.

Let us see what happens when we take **a fake point very distant (several hundred km)**, which si equivalent to change the constellation if **we keep the same time**, as we did for the results that we present here. Changing the constellation is not necessary. The experiment where we

have a fake point very far with the same constellation has not been carried out. In this case there is a high risk of being in a situation analogous to the first situation: the receiver will not prefer the spoofing signal before it has a substantial power difference.
Table 4 shows the results obtained in tracking mode, the acquisition not having any significant difference with the first case.

Table 4 – Spoofing with far fake point

Tracking					
CS/SS (dB)	-6	-8	-10	-15	-20
Noise increase (dB)	<1dB +N	<1dB+N	1dB+N	Y	Y

The change from the real signal to the spoofing one occurs for 15 dB of power difference, so for a value slightly higher than for a point closer with a different constellation. For a point farther, the change of constellation seems to facilitate the effectiveness of the lure.
In summary of this section:

- In acquisition mode, 8 dB of difference is enough to spoof the receiver.
- In tracking mode, spoofing necessitates a difference of power of 26 dB.
- By changing constellation, this threshold is reduced to 10 dB.
- By taking a very distant "fake" point, it is reduced to 15 dB.

As a conclusion, a spoofer would rather use a far "fake point" and a different constellation.

4.3 Tests on the navigation system of a drone

To conclude, we will present a result that seems significant: a scenario of GPS spoofing for a standard system of navigation of drone.

We use for this a custom made drone by the company UAVIA. Its frame is a DJI flamewheel 550 (F550) hexagon with a 55 cm diagonal motor-motor, equipped with 960 Kv E305 brushless motors. A Dropix controller containing the ardupilot firmware. The GNSS receiver is a μ-blox neo M8T chipset supporting GPS / GLONASS. Missions are planned using the Mission Planner navigation software. Figure 10 shows the drone in question.

Figure 10 – UAV used for test

The advantage of this custom made drone is that it is possible to directly connect an external antenna (or a signal generator) to the input of the GNSS receiver. Thus it is possible to test the behavior of the receiver without radiating to the antenna of the drone. The following experimental set-up is carried out (Figure 11):

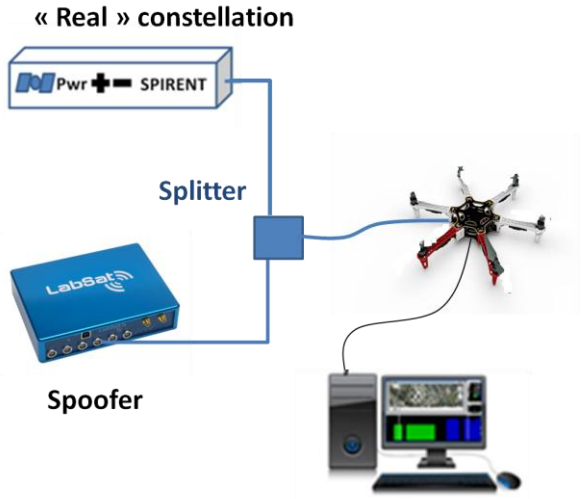

Figure 11 – Experimental Setup

When the drone is supposed to take off, the GNSS receiver calculates the position given by the Spirent generator which represents the real constellation. This position does not move. The Labsat represents here the decoy signal which is activated during the flight scenario. Here we use the same constellations (GLONASS and GPS) at about the same time on the same day for the decoy and for the real constellation. In figure 11, we see that we have removed the propellers of the drone. This is an obligation since the drone cannot fly while it is connected by wire to the signal generator and the Labsat! How to characterize the influences of the spoofing signal on the behavior of the navigation system? We concluded that the most relevant was to look at the commands the navigation software sends to the engines. This gives an idea of the speed vector that the drone is trying to give itself. It remains to define significant scenarios. The two chosen scenarios are described in figure 12.

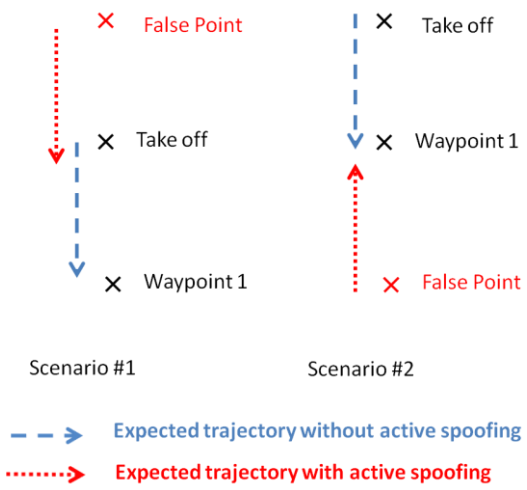

Figure 12 – Scenarios of flight missions

In fact, during the scenarios, the GNSS receiver of the drone can only give two positions: the point of take-off or the fake point given by the spoofer. The behaviour of the navigation software will depend of which position the receiver gives, and what where is the targeted waypoint. After the take-off phase, the drone activates its engines to go to the first waypoint.

In the first scenario, given the configuration of the three points (take off, fake point and waypoint), it is expected that activation of the decoy will not cause a major variation in the velocity vector, and hence in engine controls. Indeed, that the drone believes to be at take off position or at the fake position, the direction to be taken is the same. For Scenario 2 it is quite different. We should logically see a reversal of the engine controls because the spoofing signal tells the drone that it has overtaken its first waypoint without reaching it.

It is not shown here, but it has been possible to check for the two scenarios that the decoy points are calculated when the spoofing is active, and that the point is transmitted to the navigation system of the drone. We therefore test the behavior of the automatic navigation system according to the variations of the GPS data.

Figures 13 and 14 give the results of the commands sent to the 6 drone engines during the two scenarios (the value of the units on the y axis has a meaning specific to the control software. These values are interesting for us only to compare the Engines between them).

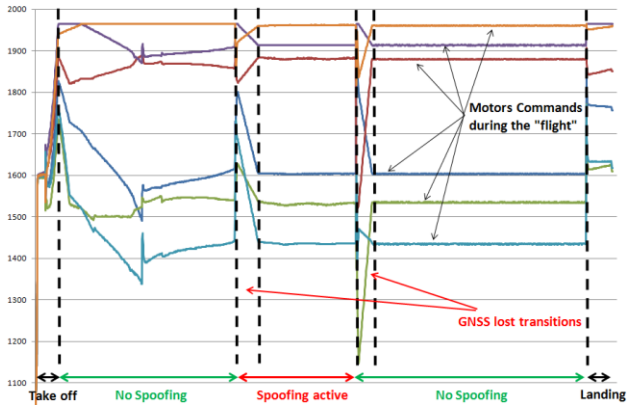

Figure 13 – Motors Command for Scenario 1

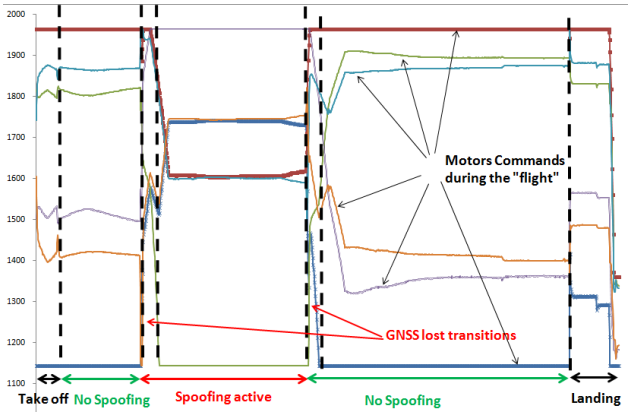

Figure 14 – Motors Command for Scenario 2

The start of the curves corresponds to the take-off phase. The almost steady state that is observed then corresponds to the engine controls that the navigation system sends to reach the first waypoint. Then there is a transition phase of fifteen seconds during which the drone has no GPS point (it maintains its engine speed nonetheless). Then it is under the influence of the lure for about 50 seconds. The engine controls vary greatly in Scenario 2 and practically not in Scenario 1, which confirms what was expected about the operation of the navigation system.

When the influence of the spoofer disappears, we again have a transition of about 15 seconds before resuming the same motor controls that we had at the beginning (it is more or less identical according to the engines, this difference comes probably of the direction that the drone measures with its compass). The end corresponds to the automatic landing which precedes the engines cutoff.

During Scenario 1, engines receive identical commands before, during and after the spoofing phase. This means that for navigation system, the direction to be taken is always the same. For Scenario 2, the commands are almost identical before and after the spoofing phase and they are very different during. The analysis is quite simple: when the drone is under the influence of the spoofer, it changes its controls to adapt its speed and direction to the new point where it believes itself to be. Once the spoofer is off, the GNSS receiver indicates that it is located to its old position, and as its mission is always to go towards the first waypoint, it resumes the behavior that it had at the beginning, with a few differences (it can be seen in figure 14 that one of the engines does not receive exactly the same command than before).

It is difficult to take the analysis further these findings. To validate definitively the simulations, it would be necessary to be able to carry out experiments on a flying drone. GNSS regulation prevent from going further than these laboratory experiments.

5 CONCLUSION

The experiments showed, on the one hand, the levels of signals required to take control of a GNSS receiver and on the other hand the almost exclusive dependence of the automatic navigation system towards the point given by

the GNSS receiver. From there, one can conclude that there is no need to be as "subtle" as [Shepard & Al 2012] to take control of the GNSS receiver of a civilian drone. A simple recorder / replayer of GNSS signals of a few thousand euros is enough.
It can nevertheless be said that it would not be very complicated for the drone to at least perceive that it is under the influence of a coarse decoy. A simple analysis of the clock bias would be enough to detect the fake signals. The change in the covariance of the Kalman filter could activate some emergency procedure. But at present nothing is really deployed for small civilian drones, and when it is the case, a question remains: what behavior the drone must adopt when it knows it is under the influence of a spoofer? Take altitude, warn its base, etc. A question that is far from obvious, and the other problematic, which consists of finding ways to counter effects of a spoofing signal, this is a completely different story of quite another complexity.

ACKNOWLEDGMENTS

We would to thank Mr Raphaèl Roman who have opered the drone during the experimentation.
We would like to thank Mr Alain Caignault and SPIRENT Company for their support by lending us the GSS generator.
We would also like to thank the partners of the ANGELAS consortium: the ONERA, the CEA, Thales Communication and Security, EDF, Exavision and l'Institut de Criminologie et de droit pénal de Paris.

REFERENCES

[Caratori & Al 2003] Caratori J., François M., Samama N., « Upgrade Simulation Results for the R1S approach », GNSSS, April 2003, Graz, Austria.

[Tippenhauer & Al 2011] Nils Ole Tippenhauer, Christina Pöpper, Kasper B. Rasmussen Srdjan Capkun, CCS '11 Proceedings of the 18th ACM conference on Computer and communications security Pages 75-86 ACM New York, NY, USA ©2011.

[Broumandan & Al 2015] Ali Broumandan, Ali Jafarnia-Jahromi, Gérard Lachapelle, "Spoofing detection, classification and cancelation (SDCC) receiver architecture for a moving GNSS receiver", GPS Solut (2015) 19:475–487

[Larcom & Al 2013] Larcom, J.A., Hong Liu, "Modeling and characterization of GPS spoofing" Technologies for Homeland Security (HST), 2013 IEEE International Conference, 2013, Pages: 729 – 734.

[Kim & Al 2012] Tae-Hee Kim, Cheon Sig Sin, Sanguk Lee, "Analysis of effect of spoofing signal in GPS receiver", 12th International Conference on Control, Automation and Systems (ICCAS), Oct. 17-21, 2012, Jeju Island, Korea

[Shepard & Al 2012] Daniel P Shepard, Jahshan A Bhatti, Todd E Humphreys, Aaron A Fansler, "Evaluation of smart grid and civilian UAV vulnerability to GPS spoofing attacks", Proceedings of the ION GNSS Meeting Nashville, TN, 2012

[Giray 2013] Sait Murat Giray, "Anatomy Of Unmanned Aerial Vehicle Hijacking With Signal Spoofing", 6th International Conference on Recent Advances in Space Technologies (RAST), pages 795 – 800, June 12-14, 2013, Istanbul, Turkey.

[Kaplan] Kaplan E. & Hegarty C., "Understanding GPS Principles and Applications", Artech House, 2006, 2nd Ed.