Journal of Aerospace Technology and Management
ISSN: 1984-9648
secretary@jatm.com.br
Instituto de Aeronáutica e Espaço
Brasil

de Abreu Faria, Lester; de Melo Silvestre, Caio Augusto; Feitosa Correia, Marcelino Aparecido

GPS-Dependent Systems: Vulnerabilities to Electromagnetic Attacks

Journal of Aerospace Technology and Management, vol. 8, núm. 4, octubre-diciembre, 2016, pp. 423-430
Instituto de Aeronáutica e Espaço
São Paulo, Brasil

doi: 10.5028/jatm.v8i4.632

GPS-Dependent Systems: Vulnerabilities to Electromagnetic Attacks

Lester de Abreu Faria[1], Caio Augusto de Melo Silvestre[1], Marcelino Aparecido Feitosa Correia[1]

ABSTRACT: The GPS is a satellite navigation system that provides location and time information. Such a system currently supports critical applications for military, civil and commercial users worldwide and is accessible to any operator by using a single GPS receiver. However, although being too dependent on GPS signals, just a few of these applications present some kind of countermeasure to electromagnetic attacks, showing a high level of vulnerability to intentional attacks. In this paper, we pose questions and situations related to security and vulnerability of different kinds of platforms/vectors and systems which directly afflict the situational awareness of operators. Experiments were made with different general GPS receivers as a function of distance and incidence angle, showing that they fail to work even at low jamming powers (−25 and 0 dBm at 10 m). More complex GPS systems, such as aeronautical receivers, were also tested, losing completely the tracking at −30 dBm, when a 0° (levelled) and 10 m far electromagnetic jamming signal is incident on its antenna. A specific open source, free software (JammPy) allows extending these experimental results, providing a roadmap and estimating how much jamming power is necessary to cause damage to these systems.

KEYWORDS: Aerospace, Electronic warfare, GPS, Jammer, GPS-dependent systems.

INTRODUCTION

The Global Positioning System (GPS) is a satellite navigation system that provides location and time information in all weather conditions and at any position where there is a line of sight to 4 or more GPS satellites (The Library of Congress 2011). Such a system supports critical applications for military, civil and commercial users worldwide, having the US government as its main sponsor. It shows itself accessible to any operator by using a single GPS receiver.

Currently, a series of applications are developed and supported primarily by this "tool", becoming highly dependent of it. They are called GPS-dependent systems, which include different tracking, encryption and navigation systems. GPS applications, such as transfer time, traffic signal timing and synchronization of cell phone base stations use the cheap and highly-accurate GPS infrastructure. However, although being essentially dependent on the GPS signals, just a few of them present some kind of countermeasure to electromagnetic attacks (jamming), becoming highly vulnerable to them.

Considering the fundamentals governing the operation of such a system, it is relatively simple to interfere with GPS signals, being either the military or a civilian. The effectiveness of interference (jamming effectiveness), depending on the distance and power of the equipment, is also quite simple to calculate, making the dimensioning of a jammer system an easy and accessible task for the majority of the population. In general, jammers can be used against any radio communication signals, whether being GPS signals, Wi-Fi signals and/or communication between mobiles. Despite being illegal in different countries, projects teaching how to build this kind of jammers are easily

[1] Departamento de Ciência e Tecnologia Aeroespacial – Instituto Tecnológico de Aeronáutica – Divisão de Engenharia Eletrônica – São José dos Campos/SP – Brazil.

Author for correspondence: Lester de Abreu Faria | Departamento de Ciência e Tecnologia Aeroespacial – Instituto Tecnológico de Aeronáutica – Divisão de Engenharia Eletrônica | Praça Marechal Eduardo Gomes, 50 – Vila das Acácias | CEP: 12.228-900 – São José dos Campos/SP – Brazil | Email: lester@ita.br

Received: 03/01/2016 | **Accepted:** 07/19/2016

found on the Internet. This is where the vulnerability of "GPS-dependent" devices comes from.

In a recent past, GPS vulnerability has been demonstrated in different episodes. In 2010, 2011 and 2012, South Korea suffered many blockages originated in North Korea. As a countermeasure to such interference, an integration of GPS with Enhanced Long Range Navigation (eLoran) was used (Lee 2013). Another incident was demonstrated in December 2011, when Iran surprised the world imposing a controlled landing to a drone RQ-170 Sentinel. It is supposed that the communication link between the control station and the aircraft was jammed, and then the GPS receiver was subjected to spoofing (Petersonm 2011).

THEORETICAL CONCEPTS

Jamming is defined as "the emission of radio frequency with enough power and with the needed features to avoid, in a given area, the receivers to track GPS signals" (Oonincx and van der Wal 2014). The low power of GPS signals (around −160 dBm on the Earth's surface) allows the jammer to be effective even at low power levels, making relatively simple and cheap to be realized. Various efficient jammers are available and cost about $ 1,000, being capable of generating 100 W of power (Carroll 2003). This power is sufficient to provide a high operation distance, as will be seen next.

Meaconing refers to the process of interception and retransmission of a signal. Considering GPS signals, a device receives the signal, amplifying and retransmitting it. The target receiver receives the original signal and the retransmitted one. Once the malignant signal arrives with higher power, the target processes this signal as the true one, thereby providing information of positioning, navigation and time corresponding to the information of the malicious transmitter (Landry *et al.* 1998).

Finally, the spoofing occurs when a false PNT information is inserted into the target receiver, which is unable to identify the attack. Although this technique is more complex, it constitutes a real threat to the current military and civil operations.

The Friis' Transmission Equation gives the power received by an antenna, under idealized conditions, given another antenna some distance away and transmitting a known amount of power. It serves as a good approximation for estimating signal levels through free space, considering the main factors that influence the propagation. It is considered just a simplified equation because it does not consider the atmospheric attenuation (or the path loss) and eventual influences of clouds and rain. It can be written as:

$$P_r = \frac{P_t A_{ef}}{4\pi(R)^2} = \frac{P_t \lambda^2}{(4\pi R)^2} = G_t G_r \frac{\lambda^2}{(4\pi R)^2} \qquad (1)$$

or, in dB:

$$P_r = P_t + G_t + G_r + 20\log_{10}\frac{\lambda}{4\pi R} \qquad (2)$$

where: G_t and G_r are the gains (with respect to an isotropic radiator) of the transmitting and receiving antennas, respectively; P_t is the transmitted power; A_{ef} is the effective area of the receiving antenna; R is the distance between antennas; λ is wavelength of the carrier.

Thus, based on Eq. 1, it can be seen that, not considering path loss, the power density that reaches the GPS receiver is inversely proportional to the square of the distance (R) of the jammer antenna to the GPS antenna. If a more complex propagation equation must be considered, Eq. 2 becomes:

$$\begin{aligned} P_r = P_t + G_t(\theta_t, \phi_t) + G_r(\theta_r, \phi_r) + \left(\frac{\lambda}{4\pi R}\right)^2 \dots \\ \dots\left(1 - |\Gamma_t|^2\right)\left(1 - |\Gamma_r|^2\right)a_t . a_r^*|^2 e^{-\alpha R} \end{aligned} \qquad (3)$$

where: $G_t(\theta_t,\phi_t)$ is the gain of the transmitting antenna in the direction (θ_t,ϕ_t); $G_r(\theta_r,\phi_r)$ is the gain of the receiving antenna in the direction (θ_r,ϕ_r); Γ_t and Γ_r are the reflection coefficients of the transmitting and receiving antennas; a_t and a_r are the polarization vectors of the transmitting and receiving antennas; α is the absorption coefficient of the intervening medium.

TARGET APPLICATIONS (SCOPE)

Although being originally a military project, the GPS is currently considered a dual-use technology, having become a widely used tool in trade, scientific applications, monitoring and surveillance.

Many civil applications use one or more of the 3 basic components of GPS (absolute location, relative movement and transfer time). Among these, some applications may be highlighted:

1. Autonomous vehicles, Unmanned Aerial Vehicles (UAVs) or drones: location and routes.
2. Cell-phones: clock synchronization allows the transfer of time, being fundamental to the synchronization of its spreading codes with other base stations (± 10 s) (National Institute of Standards and Technology 2011).
3. Navigation: designation of targets as well as troop and supply coordination (Sinha 2003).
4. Tracking targets: various weapons systems use GPS to track potential ground and aerial targets before setting them as hostiles. Such weapons systems transfer the coordinates of targets for high-performance guided weapons.
5. Missiles and projectiles guidance: GPS allows accurate pointing and guidance of different military weapons, including ICBMs, cruise missiles, precision-guided munitions and artillery projectiles (GlobalSecurity.org 2007).

Among the previously mentioned applications, the items 1, 2 and 5 may highly affect complex and high added-value military systems.

DRONES

Also known as (UAVs) or Remotely Piloted Aircraft (RPA), the flight can be remotely controlled by a pilot on the ground in real time or a route where the vehicle will fly can be defined in advance, based on GPS coordinates. There are a variety of shapes, sizes, configurations and features, depending on the target applications of the drone. They have 2 communication systems (How to kill… Date unknown):

- Radio line-of-sight: in the military C-band of 500 – 1,000 MHz, which is vulnerable and can be jammed with a simple radio.
- Satellite communications: in K_u band from 10.95 to 14.5 GHz, where the satellite may be jammed (uplink-band: from 13.75 to 14.5 GHz; downlink band: from 10.95 to 12.75 GHz).

The satellite communication system generally uses the same technology used by civil applications, except the encrypted systems. Once it is possible to jam both communication links, as suggested earlier, the operator is unable to control the aircraft, flying until colliding or the fuel is over. Radio frequencies in the C-band, in particular, are used during takeoff and landing, letting the drone to be an easy target.

JOINT DIRECT ATTACK MUNITION

Joint Direct Attack Munition (JDAM) is a guidance kit that enables the conversion of unguided bombs or “dumb” bombs into “smart” munitions. JDAM-equipped bombs are guided by an integrated inertial guidance system coupled to a GPS receiver, giving them a published range of up to 15 nautical miles (28 km). These can range from 500 pounds (227 kg) to 2,000 pounds (907 kg) (Hansen 2006). When installed on a bomb, they are called Guided Bomb Unit (GBU). The key components of the system consist of a tail section with aerodynamic control surfaces, a (body) strake kit as well as a combined inertial guidance system and GPS guidance control unit.

SAFE COMMUNICATIONS NETWORK

The communications network stations need to be synchronized to function properly. The more precise the synchronization, the smallest is the loss of information or the presence of noise. In modern synchronization systems, the time information coming from GNSS is generally used due to its accuracy and reliability.

Some systems automatically synchronize with the GPS-time, as it is the case in many civil systems. However, other systems allow the user to enter an arbitrary time information, which becomes more effective against GPS interference, if used correctly.

MATERIALS AND METHODOLOGY

Firstly, in this research, electromagnetic jamming was realized onto general receivers, such as automotive GPS and mobile phones. These experiments focus on a validation of the method and of the experimental setup, besides assessing the robustness of different receivers to jammer.

Such experiments were carried out outdoor and with the receivers vertically positioned. Distances from the radiating antenna of 10 m, with incidence angles of −10°; 0° and +10°, were measured. Finally, a jamming test at 20 m and 0° was also conducted. The power of the radiated signal was gradually increased at intervals of 3 min to allow a stabilization of the signals and the acquisition time of the receivers.

In all cases, signals generated by the jammer compete with the ones from the GPS satellites, reproducing the real environment. The experimental setup is composed of (Fig. 1):

- Signal Generator Agilent E8257D.
- DHR antenna 0118.

- SMA coaxial cable.

Two different receivers were tested:

- Cell phone Samsung Galaxy S3, with the "GPS Test" App, in order to monitor the available satellites, parameters of the coordinates and the date/time group.
- Automotive receiver (Foston).

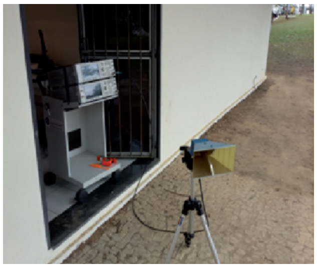

Figure 1. Experimental setup for general GPS receivers jamming.

Once assessed all possible situations for general GPS receivers, the next step was to build an experimental setup for assessing aeronautical GPS receivers. For safety reasons, data relating to aircraft and used equipment are not detailed in this paper.

The aircraft was placed outside the flight hangars where a direct line of sight from the jamming antenna to the receiving GPS antenna and to the GPS satellites would be possible. Two different GPS systems could be assessed: a stand-alone and a more complex integrated one, composed of GPS/inertial/radio-altimeter. Both work independently (including different antennas) and provide good conditions to evaluate the efficiency of the jamming system.

The integrated GPS system provides 3 independent solutions (Inertial Navigation System pure — INS, GPS pure and GPS/INS combined) simultaneously. It is possible to continuously monitor the performance of each one of the solutions, calculating a figure of merit (FOM) associated with the expected error. Such features were used as a database for this research.

An initial alignment was carried out in both systems and, after a full alignment, the initial coordinates reported by the aircraft system were presented: lat 23°13.34′S; long 45°51.96′W, as well as the airfield altitude (São José dos Campos Airport – SBSJ) of 2,040 ft, coincident in both systems.

The experimental setup, the used equipment and the jammer power procedures were the same as those mentioned for general GPS receivers tests. The receiving and transmitting antennas were positioned at a distance of 10 m and at angles of 0° and −6° in respect to the antenna of the aircraft, as shown in Fig. 2, where the type of aircraft is merely illustrative.

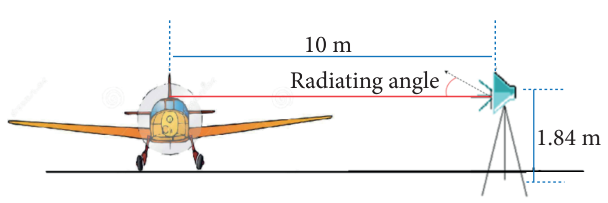

Figure 2. Experimental setup for aeronautical GPS receivers jamming.

Jamming was performed using narrowband signals without modulation, interfering in the C/A signal of the L1 carrier (1,575.42 MHz). For a better comparison of the effects of the jamming, the stand-alone GPS position was referenced to the non-directional (radio) beacon of São José dos Campos (NDB SJC) on the results of the first test and to the airfield of Lagoa Santa (SBLS) in the second test. These benchmarks are at 1 and 240 NM of the actual position of the tested equipment, respectively.

EXPERIMENTAL RESULTS

The first tests focused on general GPS receivers, where an automotive GPS receiver and a cell phone were assessed.

As could be confirmed in the first experiment, both receivers (Samsung S3 cell phone and Foston automotive receiver) are vulnerable at fairly low powers, when jammed by an antenna placed 10 m far and at an angle of 0°.

The automotive GPS receiver (Foston) proved to be more sensitive, once at −20 dBm it stopped receiving signals from all available satellites. It clearly demonstrates a high vulnerability and no countermeasures of any kind for such interference. Besides, since GPS systems need at least 4 GPS signals to work properly, it is possible to conclude that, at −25 dBm, it was not reliable anymore, because, at this jammer power, only one satellite signal could be received.

The Samsung S3 receiver showed to be more robust, acquiring 5 satellites up to −5 dBm and, therefore, generating a reliable location information. However, with an interference of 0 dBm, it also succumbed, losing all signals.

In the second part of the experiment, the number of visible satellites (in line of sight with the GPS receiver) increased for both receivers. Increasing the distance between the jamming antenna and the GPS receiver to 10 m far, it could be perceived that the Foston receiver needed approximately more 10 dB to cancel all the received GPS signals, agreeing with the expected behavior related to Eq. 1.

On the other hand, Samsung S3 cell phone presented an unexpected behaviour, since all the GPS signals were cancelled with a power lower than that used when the jamming antenna was 10 m far from the GPS antenna. This can be easily explained because the weather conditions noticeably deteriorated during the experiment, which has attenuated the signal from the GPS satellites, letting them weaker and then easier to be cancelled by the jammer. It can be supported by Eq. 3, in which the parameter α refers to this kind of signal loss. Thus, although at the beginning of the experiment there were more visible satellites, their signal arrived to the ground considerably weaker, making them easier to be cancelled by a jammer.

In the third experiment, it could be verified the sensitivity of the receiver to jamming with angles of incidence different from 0°, 10 m far, being the case in a real attack coming from the ground or from a flying vector. Firstly, it was simulated a jammer illuminating the receiver from the ground, at an angle of –10°.This change did not considerably affect the Foston receiver, which had its signal cancelled at the same radiated power (maybe some small differences of power between –25 and –20 dBm). This suggests that the antenna radiation diagram of this receiver presents a similar sensitivity to radiated signals coming from the ground or from leveled jamming antennas.

On the other hand, the Samsung S3 cell phone needed 5 dBm instead of 0 dBm to have the signal cancelled. This result suggests that this antenna radiation pattern is more directed to the upper hemisphere, presenting a large attenuation for the lower one.

Therefore, depending on the radiation pattern of the antenna, installed in the target vector, more or less power will be necessary to cancel the GPS signal. It is always necessary to evaluate the target and the antenna before going to an actual jamming procedure.

Finally, in the fourth experiment, a jammer illuminating the GPS receiver from the upper hemisphere was simulated at an angle of 10°, 10 m far. The Foston receiver showed the same radiation power profile for the cancelling of the GPS signals than the ones seen in the previously experiments, showing an antenna radiation pattern very isotropic in all directions from –10° to 10°.

Since the cell phone Samsung S3 showed the extinction of the signal with a very low radiated power (–20 instead of 0 dBm), it can be concluded that the sensitivity of this equipment is much higher for the upper hemisphere. A simple comparison of both radiation patterns leads to the scheme in Fig. 3, where the left radiation pattern suggests the one from Foston automotive GPS and the right one leads to the Samsung S3 radiation pattern (vertical profile).

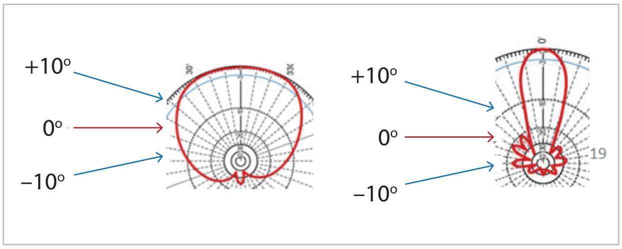

Figure 3. Suggested profiles of the radiation pattern of the tested devices.

After testing the general application receivers, some tests were performed in aeronautical GPS devices, including a stand-alone GPS and an integrated solution (GPS/inertial/radio-altimeter — GPS+IMU-RALT).

In a first test, an incidence angle of –6° was used between the jamming antenna and the aircraft antenna, while, in a second test, an angle of 0° between them was used. The results can be seen in Tables 1 and 2.

In Tables 1 and 2, it is possible to evaluate, for different jamming powers, the threshold power, the integrated GPS solution error (GPS solution) and the stand-alone GPS error.

Concerning specifically to the stand-alone GPS system, it showed to be highly vulnerable, once, in both tests, even using very low jammer power, the system lost the detection, showing very high errors before that.

In the first test, it can be seen that, at –50 dBm of jamming power, the receiver already indicates a wrong position (based on SJC benchmark), although keeping the initial position. This error gradually increases with the increasing in the jamming power.

In the second test, when the jamming signal started to be radiated, the receiver indicated that the aircraft was moving with a ground speed (GS) of 50 kt. The position indication did not change too much when compared to the first test indications. Figure 4 shows the displacement of the coordinates of the GPS relatively to the jamming power.

At the early stages of the experiment, the increasing power of the jamming signal apparently did not influence significantly the position indications. However, as the power increases above –85.9 dBm (which may be considered a threshold power for an incidence angle of 0°), considerable errors could be perceived. Figure 4d shows the final position indicated by the system, with a power of –40 dBm. From –30 dBm on, the receiver was unable to provide any coordinates information.

Table 1. First test results (angle of –6° between jammer and GPS antenna).

Jammer power (dBm)	Power at the GPS antenna (dBm)	Integrated GPS solution error (m)	Stand-alone GPS (present position) distance from the NDB SJC
-60	- 115.96	25	1 NM — Initial position
-50	- 105.96	1,000	2.6 NM — Initial position
-40	- 95.96	75	3.6 NM — Initial position
-30	- 85.96	500	4.8 NM — lat 23°09.81′S; long 45°54.63′W
-20	- 75.96	500	8.0 NM — lat 23°08.42′S; long 45°59.61′W
-10	- 65.96	500	No present position (lost coordinates)

Table 2. Second test results (angle of –0° between jammer and GPS antenna).

Jammer power (dBm)	Power at the GPS antenna (dBm)	Integrated GPS solution error (m)	Stand-alone GPS (present position) distance from the NDB SJC
-60	- 115.9	50	240 NM — lat 23°13.04′S; long 45°51.92′W — GS 50 kt
-50	- 105.9	50	232 NM — lat 23°13.00′S; long 45°51.92′W — GS 50 kt
-40	- 95.9	700	240 NM — lat 23°12.15′S; long 45°51.93′W — GS 50 kt
-30	- 85.9	200	No present position (lost coordinates)
-20	- 75.9	500	No present position (lost coordinates)
-10	- 65.9	500	No present position (lost coordinates)

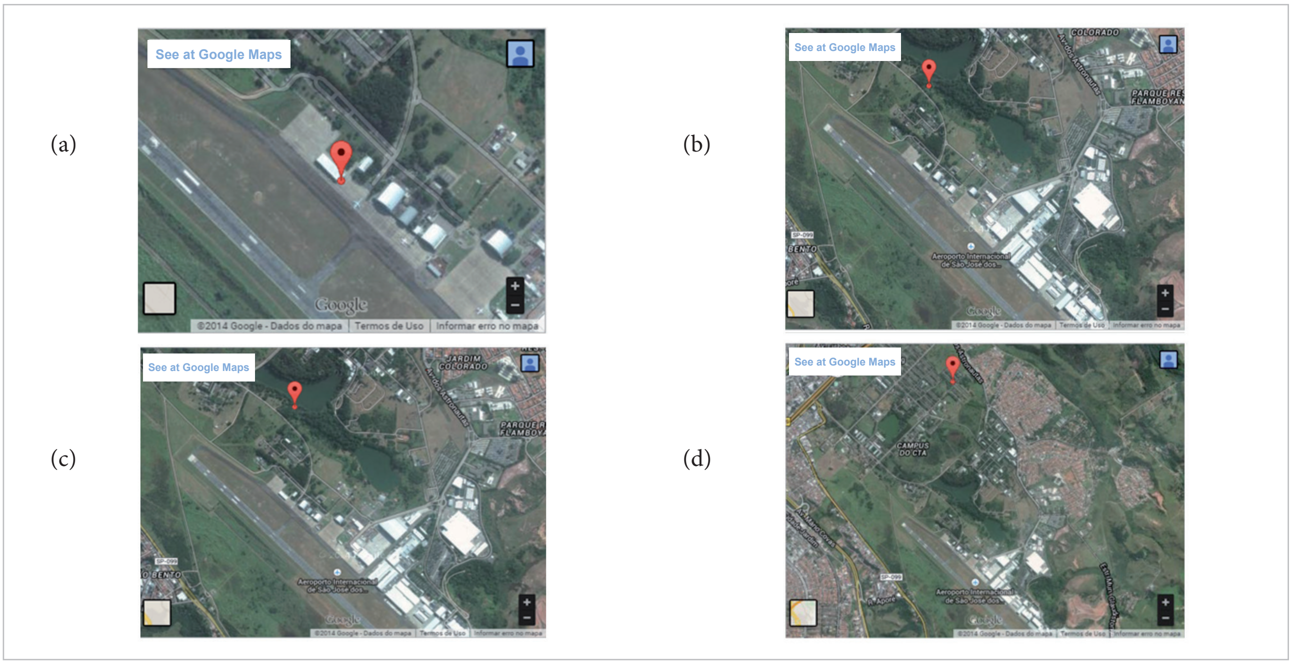
(a)
See at Google Maps
Google
©2014 Google - Dados do mapa | Termos de Uso | Informar erro no mapa
(b)
See at Google Maps
(c)
See at Google Maps
(d)
See at Google Maps
Aeroporto Internacional de São José dos...
CAMPUS DO CTA

Figure 4. Indicated GPS position. (a) Actual; (b) –60 dBm; (c) –50 dBm; (d) –40 dBm, for 0° of incidence angle between the jammer and the GPS antennas.

Improving the robustness of the GPS system and testing the integrated solution (which is used in various actual systems, as the ones previously mentioned in this article), the same tests were conducted. In this case, the base parameter for the evaluation was the FOM, highlighting that the GPS position solution mode was active. This parameter increased as the jamming signal increased. Error spikes (outliers) could be seen during the tests, although no explanation was found untill the final version of this article.

Some additional tests are important to evaluate these outliers, but the preliminary results are those presented in Tables 1 and 2.

Concerning the variation of the incidence angle, the error showed to be different for both tests. Figure 5 shows the average calculated error (integrated GPS solution) for different jamming signal levels.

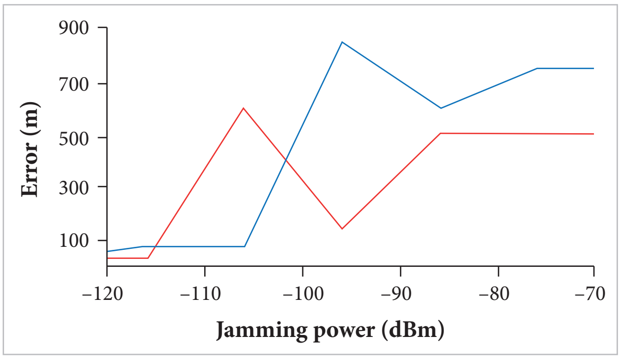

Figure 5. Average error for the GPSA integrated solution. Results for an incidence angle of −6° (red); Results for 0° (blue).

Based on Fig. 5, it is possible to conclude that, with an incidence angle of −6°, the error increases rapidly for lower jamming powers and then stabilizes at 500 m. For an incidence angle of 0°, the error remains lower than that up to −100 dBm, approximately, and then stabilizes around 750 m. These results suggest that, even using complex GPS systems, considerable errors may be inputted in real systems.

SIMULATION RESULTS

Based on the previously presented results, a very simple analysis was performed in order to estimate the necessary power to damage the control system of GPS-dependent devices. For that, it was considered a flying vector (drones, JDAM, aircrafts or safe communications network) with a specific altitude (in feet) and distance (in meters) from the jamming antenna. The used threshold power was −30 dBm, found experimentally in the previous experiments. This threshold power can be considered the worst case, because, with less than −30 dBm, the GPS systems already present a loss. It was adopted just to have an idea of a jammer efficiency. The atmospheric transmittance was considered 100%; the gains of the jammer antenna and the GPS antenna are the same as those evaluated for the aeronautical GPS receiver. The results are based on the Eq. 2 of this article. Figure 6 depicts the 3-D solution for this kind of interference.

In Fig. 6, it is possible to see the necessary jamming power for a complete extinction of the GPS signal on the receiving antennas, where Jamming power levels below 1 W are presented in green, while those above 5 W are shown in red. Powers between these values are presented in blue. All calculi were performed in an open source and free software called JammPy, specially developed for this research. Based on the threshold power (in dBm) and the distance (in meters) at which this power is efficient, it is possible to generate 3-D graphs, like the one presented in Fig. 6, for any range of altitudes and distances, allowing to evaluate and estimate the necessary jamming power for very specific targets and flight profiles.

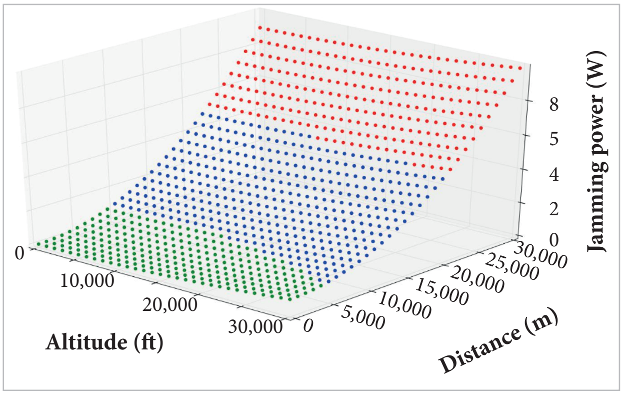

Figure 6. Necessary jamming power for a complete extinction of the GPS signal in aeronautical vectors, considering the distance and the altitude from the jamming antenna.

From the graph, one can conclude that, even for vectors at a high altitude (as high as 30,000 ft) and in a high distance from the jamming antenna (30 km), it is possible to have a successful interference with relatively low jamming powers (less than 10 W). These results show that GPS jamming is a very dangerous threat to any kind of GPS-dependent system.

CONCLUSIONS

GPS supports critical applications for military, civil and commercial users worldwide. Just a few of these applications present some kind of countermeasure to electromagnetic attacks, showing a high level of vulnerability to intentional attacks. Experimental results of jamming on general receivers, including cell phones and automotive GPS, show that all of them present a high vulnerability to this kind of interference, losing the satellite GPS signal at a fairly low jamming power. At −25 dBm, no more satellites can be seen by the automotive GPS under an attack 10 m far from it. The same situation occurs with a cell phone GPS, but at 0 dBm. The experiments were repeated at different incidence angles and distances, showing variable behaviors for the receivers and suggesting that, depending on the target, different powers and strategies of interference must be applied.

Concerning more complex systems, such as the aeronautical ones, it was possible to test 2 different and independent systems: a stand-alone GPS receiver and an integrated solution, composed of a GPS+IMU-RALT. Both GPS systems were jammed and lost their signals at a relatively low jamming power, showing a high vulnerability to electromagnetic attack. Different distances and incidence angles were tested showing that the stand-alone GPS is more vulnerable to jamming, although the integrated solution also presents a high error at low jamming power.

Thus, based on the experimental results, a software was developed (JammPy) in order to dimension the necessary power to jam a flight vector. The threshold power and distance at which the experiment was run are the input values for the calculus of the jamming power to interfere with a vector, as a function of distance and altitude. These conclusions allow to generate a danger area (map) where any kind of vector can be jammed with a specific jamming device (power generator and antenna). This can be used to develop doctrine to attack or to dimension a safe zone for our vectors.

Finally, it must be highlighted that the presented results lead to a high concern for the most part of countries that use GPS-dependent systems embedded on their terrestrial and aerial vectors, because less than 1% of defense communications, nowadays, has some kind of countermeasure to any type of electromagnetic attack, even the most simple ones (How to kill… Date unknown; Thompson 2010; ABC 2000).

AUTHOR'S CONTRIBUTION

Faria LA conceived the idea and wrote the main text, providing the simulation. Silvestre CAM and Correa MAP performed the experiments and co-wrote the main text. All 3 authors discussed the results and commented on the manuscript.

REFERENCES

ABC (2000) Backyard satellite jammers concern US Airforce; [accessed 2015 Feb 15]. http://www.abc.net.au/science/news/space/SpaceRepublish_120537.htm

Carroll JV (2003) Vulnerability assessment of the U.S. transportation infrastructure that relies on the global positioning system. J Navigation 56(2):185-193. doi: 10.1017/S0373463303002273

GlobalSecurity.org (2007) XM982 Excalibur precision guided extended range artillery; [accessed 2015 Mar 19]. www.globalsecurity.org/military/systems/munitions/m982-155.htm

Hansen R (2006) JDAM continues to be warfighter's weapon of choice; [accessed 2015 Feb 15]. www.archive.today/k4VX

How to kill UAVs (Date unknown); [accessed 2015 Mar 19]. http://privat.bahnhof.se/wb907234/killuav.htm

Landry RJ, Calmettes V, Bousquet M (1998) Impact of interference on a generic GPS receiver and assessment of mitigation techniques. Proceedings of the 5th International Symposium on Spread Spectrum Techniques and Applications; Sun City, South Africa.

Lee SJ (2013) GNSS vulnerability issues in Korea. South Korea: Chungnam National University.

National Institute of Standards and Technology (2011) Commom view GPS time transfer; [2015 Feb 22]. http://web.archive.org/web/20121028043917/http:/tf.nist.gov/time/commonviewgps.htm

Oonincx PJ, van der Wal AJ, editors (2014) Optimal deployment of military systems: technologies for military missions in the next decade. The Hague: T.M.C. Asser Press.

Petersonm S (2011) Iran hacked RQ-170 GPS — fooled into autopilot landing in Iran; [accessed 2014 Sept 17]. www.uasvision.com/2011/12/16/iran-hacke-rq-170-gps-fooled-in-autopilot-landing-in-iran/

Sinha V (2003) Soldiers take digital assistants to war; [2015 Feb 22]. https://gcn.com/articles/2003/07/24/soldiers-take-digital-assistants-to-war.aspx

The Library of Congress (2011) What is a GPS? How does it work?; [accessed 2015 Feb 24]. http://www.loc.gov/rr/scitech/mysteries/global.html

Thompson LB (2010) Lack of protected satellite communications could mean defeat for joint force in future war; [accessed 2015 Feb 22]. http://lexingtoninstitute.org/lack-of-protected-satellite-communications-could-mean-defeat-for-joint-force-in-future-war/?a=1&c=1171