



Journal of Aerospace Technology and Management

ISSN: 1984-9648

ISSN: 2175-9146

Departamento de Ciência e Tecnologia Aeroespacial

Faria, Lester de Abreu; Silvestre, Caio Augusto de Melo;
Correia, Marcelino Aparecido Feitosa; Roso, Nelson A.
Susceptibility of GPS-Dependent Complex Systems to Spoofing
Journal of Aerospace Technology and Management, vol. 10, e0218, 2018
Departamento de Ciência e Tecnologia Aeroespacial

DOI: <https://doi.org/10.5028/jatm.v10.839>

Available in: <https://www.redalyc.org/articulo.oa?id=309456744002>

- How to cite
- Complete issue
- More information about this article
- Journal's webpage in redalyc.org

UABM
redalyc.org

Scientific Information System Redalyc

Network of Scientific Journals from Latin America and the Caribbean, Spain and Portugal


Project academic non-profit, developed under the open access initiative

Susceptibility of GPS-Dependent Complex Systems to Spoofing

Lester de Abreu Faria¹, Caio Augusto de Melo Silvestre¹, Marcelino Aparecido Feitosa Correia¹, Nelson A. Roso¹

How to cite

Faria LA  <https://orcid.org/0000-0003-1785-446X>

Silvestre CAM  <https://orcid.org/0000-0002-8740-7625>

Roso NA  <https://orcid.org/0000-0002-7178-8224>

Faria LA; Silvestre CAM; Correia MAF; Roso NA (2018)
Susceptibility of GPS-Dependent Complex Systems to Spoofing.
J Aerosp Technol Manag, 10: e0218. doi: 10.5028/jatm.v10.839.

ABSTRACT: GPS-based systems have been widely used in different critical sectors, including civilian and military applications. Despite of being able to provide great benefits, under certain circumstances they show to be highly vulnerable to intentional interferences. In this context, this article aimed to evaluate the susceptibility of different complex GPS-dependent systems to intentional interferences, focusing on the technique known as spoofing. This technique presents a high complexity and a great potential for damaging/deceiving complex systems, besides being difficult to identify and to implement countermeasures. Complex systems, like mobile phones, automobile receivers and aircraft receivers were submitted to different levels of spoofing, in free space and in a semi-anechoic chamber, being corrupted with low power levels of interference.

KEYWORDS: GPS Receivers, Jamming, Spoofing, Vulnerabilities.

INTRODUCTION

Global Navigation Satellite Systems (GNSS) are currently used throughout the Earth, providing estimations of Position, Navigation and Timing (PNT) to all operators that have a simple GPS receiver and a line of sight to, at least, four satellites.

Considering the current existing systems, the most used one is the Global Positioning System (GPS), or NAVSTAR-GPS (NAVigation System Timing And Ranging), having the US government (Department of Defense – DoD) as its main sponsor. It was the first GNSS system fully available to the users, through the creation of a constellation of satellites. Other systems already in operation, or under development, are: the Russian GLONASS (Global Navigation Satellite System); the European GALILEO (Global European Navigation Satellite System); and the Chinese BDS (BeiDou Navigation System) (Bakker 2006). All the considerations provided here for the GPS system are extensive to the other ones, with minor modifications.

The system provides two types of positioning services: the SPS (Standard Positioning Service) and the PPS (Precision Positioning Service). The first is available to all users, regardless of the application, while the second is restricted only to DoD authorized users, being accessed via cryptographic techniques (Balvedi 2006). Unlike these kinds of GPS signals, which are encrypted and can be authenticated, the civilian ones (and those who do not have the DoD authorization) were never intended for safety- and security-critical applications.

However, currently, the GPS system supports many critical applications not only for military, but also for civilian and commercial users worldwide. Fourteen of sixteen critical sectors of the economy depend on the GPS signals (navigation, precision agriculture, financial market, communication, etc.). Besides, in military, where this dependency is not so clear, Emitters Locating Systems (ELS), Secure Communication (SC) and Multistatic Radars (MSR), which depends on the time or frequency, are also supported by those signals, becoming increasingly dependent.

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

Correspondence author: Lester de A. Faria | Departamento de Ciência e Tecnologia Aeroespacial – Instituto Tecnológico de Aeronáutica – Divisão de Engenharia Eletrônica | Praça Marechal Eduardo Gomes, 50 – Vila das Acácias | São José dos Campos/SP – Brazil | Email: lester@ita.br

Received: Nov. 11, 2016 | Accepted: May 15, 2017

Section Editor: Waldemar Leite Filho



However, as demonstrated previously in Faria *et al.* (2016), despite its complexity of design and implementation, the GPS shows to be highly susceptible to the influence of intentional malicious actions, which may lead not only to a decreased accuracy (jamming), but also to the avoidance of its use through the indication of corrupted coordinates and time (spoofing). These actions result from its high sensitivity, becoming vulnerable to high signals.

Nowadays, on internet (open sources), it is very easy to find not only jamming equipment, but also spoofing ones to buy, at lower prices than expected. Besides, several tutorials can be found on websites and YouTube, detailing how to spoof and jam vectors, especially drones. It is just to google it and one can find security experts raising alarm over online drone hacking instructions (Russon 2015).

In addition, successful spoofing experiments on standard receivers have been increasingly reported (Tippenhauer *et al.* 2011), showing that commercial off-the-shelf receivers are not able to detect such attacks. The increased availability of programmable radio platforms, as will be shown later, leads to a reduced cost of attacks and to a high vulnerability of GPS systems.

In this context, this article aims to evaluate the susceptibility of complex GPS-dependent systems to spoofing, which is shown as an advanced technique of interference, where corrupted PNT signals are transmitted to the receiver, overlaying the true GPS signals. This procedure presents a high potential of damage, so that is very difficult to identify and to countermeasure. Information on the capabilities, limitations, and operational procedures helps to identify vulnerable points and detection strategies, reasons that justify this work.

In order to illustrate the high vulnerability of such systems, it stands out the case of the US RQ-170 Sentinel. In December 2011, Iran surprised the world forcing an Unmanned Aerial Vehicle (UAV) “RQ-170 Sentinel” to have a controlled landing in Iranian territory. Figure 1 depicts the incident, not presenting accurate information of the procedures and infrastructure that Iran used to perform such task. One can only infer that the communication link between the control station and the UAV has been jammed/blocked, and the UAV GPS receiver spoofed, which forced its landing (Petersomn 2011). It is worth noting that US uses an encrypted GPS code, hindering the success of interference, but, in this case, not being sufficient to prevent the Iranian action.



Figure 1. US-RQ 170 Sentinel action, in Iran (Petersomn 2011).

THEORETICAL CONCEPTS

GPS SIGNALS

GPS system determines the user's position in real time. For that, right-circularly polarized waves are continuously emitted in three carrier frequencies, L1, L2 and L5 (respectively 1575.42 MHz, 1227.6 MHz and 1176.45 MHz), where the latter is not yet fully operational.

The carriers are BPSK (Binary Phase Shift Keying) modulated with PRN (Pseudorandom Noise) codes. The PRN code is a binary sequence, which, in addition to identifying the satellite, makes the spread spectrum signal, allowing all satellites to transmit at the same frequency. The transit time is calculated from the received signal correlated with its replica, generated in the receiver, enabling the calculation of its position. This is possible when establishing communication with, at least, four satellites.

Each transmitter is equipped with a synchronized clock, with no clock offset to the exact system time t^s , and broadcasts a carefully chosen navigation signal $s_i(t)$ (including timestamps and information on the satellites' deviation from the predicted trajectories). A receiver V located at the coordinates $L \in R^3$ (to be determined) and using an omnidirectional antenna will receive the combined signal of all satellites in range:

$$g(L, t) = \sum_i A_i s_i \left(t - \frac{|L_i^s - L|}{c} \right) + n(L, t) \quad (1)$$

where A_i is the attenuation that the signal suffers on its way from L_i^s to L , $|L_i^s - L|$ denotes the Euclidean distance between L_i^s and L , and $n(L, t)$ is background noise.

Two PRN codes modulate the L1 frequency: C/A (coarse/acquisition clear) code and the P(Y) (precision code) encrypted code. The P(Y) code is a PRN with 10.23 MHz, what leads to a length of 30 meters. On the other hand, the C/A code operates with a chipping rate of 1.023 MHz and a length of 300 m, only in L1 carrier. The C/A codes are available for civilian and military users, while the P(Y) code is for the exclusive use of the militaries (Balvedi 2006). In civilian GPS (and those which do not have authorization of the US DoD), the signals are spread using publicly known spreading PRN codes. The codes used for US military GPS are kept secret, serving for signal hiding and authentication.

Once the C/A code is open to all SPS users, it is the most widely used code in civilian and military GPS receivers, being present only in L1 signal. In addition to the PRN codes, the navigation message also modulate the carriers, including information of the broadcast ephemeris, satellite clock corrections, almanac data, ionosphere information and satellite health status.

L1 signal is defined as:

$$S_{L1} = A_p \cdot P(t) \cdot D(t) \cdot \cos(2 \cdot \pi \cdot f_1 \cdot t + \phi) + A_c \cdot C(t) \cdot D(t) \cdot \sin(2 \cdot \pi \cdot f_1 \cdot t + \phi) \quad (2)$$

where S_{L1} is the frequency of the L1 signal, A_p is the amplitude of the P(Y) code, $P(t)$ is the phase of the P(Y) code and $D(t)$ is the navigation message, f_1 is the frequency of the carrier L_1 , ϕ is the initial phase and finally A_c and $D(t)$ are the amplitude and the phase of the C/A code, respectively.

The analysis presented in the present paper is restricted to the study of the effects on the L1 carrier signals, which is the frequency used by the SPS users, the great majority of civil and military institutions outside the United States.

POWER LEVELS

The GPS system specification provides, for transmission, a power about 27 watts (or 14.3 dBw) to the C/A code in L1. The minimum received power level for the C/A code, in L1, is -160 dBw, not expecting to exceed -153 dBw (Kaplan and Hegarty 2006). These low power level signals explain the high susceptibility to intentional jamming and spoofing.

The antenna of a GPS system has omnidirectional characteristics. Its radiation pattern should provide reception of all GPS signals within the reception hemisphere of the antenna (from horizon to horizon, at all elevations). On the other hand, interfering

signals generally have low elevation angles, where receiving antennae present lower gains, on the horizon. The gain does not vary with the azimuth, but with the elevation angle, as can be seen in Fig. 2.

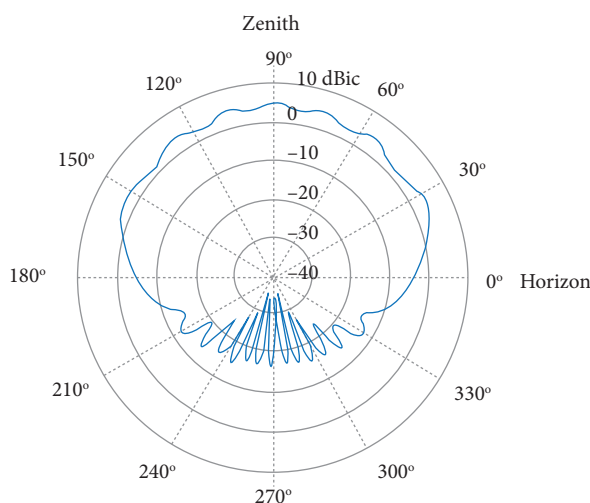


Figure 2. Typical radiation diagram of a GPS receiving antenna.

SPOOFING

Inserting false PNT information in a GPS receiver is what can be defined, quite simply, as the spoofing technique. Spoofing is a more threatening electronic attack than jamming because the targeted GPS receiver or the victim's receiver cannot detect the attack and so cannot warn users that its navigation solution is untrustworthy. This technique is quite complex and cause major damage to military and high-value civilian operations when not identified. Because of the high risk that it offers, just a few detailed information is open-access, although some of them can be found (Tippenhauer *et al.* 2011; Humphreys *et al.* 2008). Besides, equipment that allows implementing it at different levels of complexity is also available on internet and literally allows controlling the victim's GPS system.

The simplest form of spoofing, or spoofing level 1, uses a GPS signal simulator to generate a false signal, containing multiple satellite GPS signals. After generating the signal, radio frequency is radiated toward a victim receiver. The main deficiency shown in this technique is the desynchronization between the false and the true GPS signals, since they will not present the same phase. This desynchronization does not allow the processing of the false signal, so acting as noise and, if the power level is enough, it can cause the victim receiver to miss the original signal, thus acting as a simple jammer and alerting the operator to a possible spoofing (Warner and Johnston 2002).

A more efficient variation of spoofing, also known as spoofing level 2, is the one in which the attacker previously knows the position and speed of the victim receiver. This attack can be accomplished using a simulator and a portable GPS signal receiver (receiver-spoofers), which must be positioned close to the target, so that they receive the same signal. Based on this signal, the receiver-spoofers creates a false one. If this technique is performed correctly, the victim receiver will display all PNT information, based on malicious signal.

In order to conduct a spoofing task, initially a correlation between the corrupted and the original signal must be performed. When the peak of correlation of the corrupted signal is aligned with the original one, the power of malicious signal is increased. Thus, the receiver DLL (Delay Lock Loop) centralizes the false signal, taking the "control" of the victim receiver, and can generate any PNT information by the simple manipulation of the generated signal. Although this technique is highly complex, experiments show that it is possible and feasible to be implemented (Warner and Johnston 2002).

Figure 3 depicts the process of control of the receiver DLL, where it is possible to observe the correlation between the code generated in the receiver and the GPS signals (original and corrupted ones). As can be seen, after the correlation of the signals, the malicious one mocks the victim receiver, becoming the main signal provide information to the receiver.

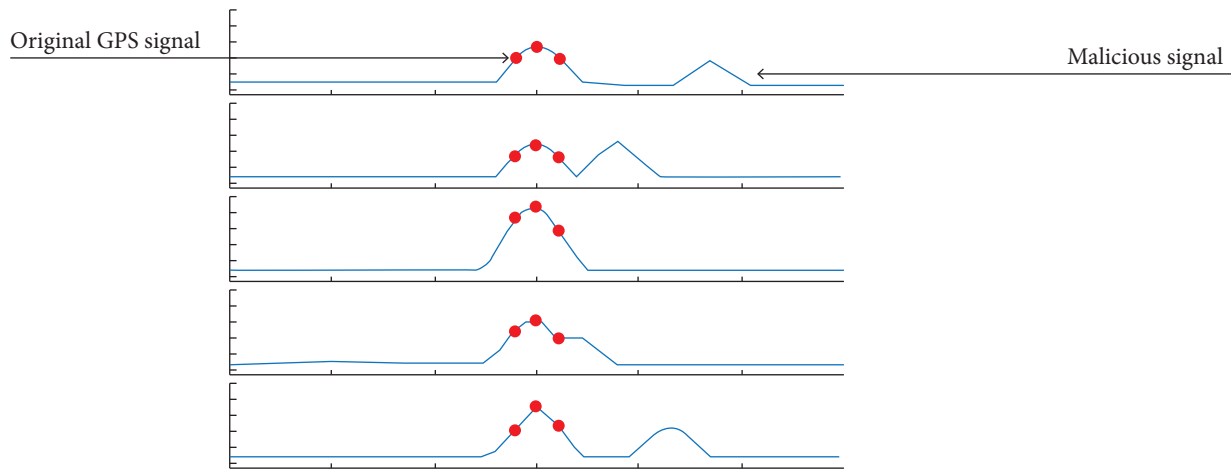


Figure 3. DLL domain.

Finally, a third spoofing technique, known as spoofing level 3, is based on a set of receivers-spoofers, in a coordinated way to remove some possible countermeasures that can be implemented based on spatial discrimination. This technique is the most complex and therefore the most expensive and difficult to achieve.

PREVIOUS RELATED WORK

In 2001, the Volpe report (John 2001) firstly identified a malicious interference in civilian GPS as a problem, writing that: “as GPS further penetrates into the civil infrastructure, it becomes a tempting target that could be exploited by individuals, groups, or countries hostile to the U.S.”. After that, spoofing attacks were treated in different publications and, in Warner and Johnston (2002), a satellite simulator was firstly used to attack a receiver mounted in another platform, being successful in taking over the victim’s satellite lock. In Humphreys *et al.* (2008), GPS spoofing signals were created by decoding legitimate GPS signals and generating time shifted copies (meaconing), which were transmitted with higher energy to overlay the original ones, what was repeated in Motella *et al.* (2010). Meaconing shows to be less expensive but generates time delays between signals (Tippenhauer *et al.* 2011).

GPS spoofing is discussed analytically in Kuhn (2004), showing that it is possible to manipulate military and civilian GPS signals by pulse-delaying, or replaying (individual) navigation signals with a delay.

These different possible models of attack require a variety of countermeasures focusing on avoiding collateral effects, what is discussed in John (2001); Kuhn (2004); Papadimitratos and Jovanovic (2008a; 2008b); Warner and Johnston (2003). In a close future, countermeasures shall rely only on modifications of the receivers, once those that could be implemented in the signals, or in the satellites themselves, have low probability of implementation, due to the high complexity.

In literature, just a few publications (Motella *et al.* 2010; Cavaleri *et al.* 2010; Ledvina *et al.* 2010; Montgomery *et al.* 2009) present experimental data on spoofing attacks, indicating a high-added value for any information concerning to this unexplored theme.

EXPERIMENTAL SETUP AND RESULTS

Aiming to check and validate the previously described concepts, some experiments were designed, addressing different levels of intentional interference (spoofing) in different kind of receivers, from the simplest (automotive receivers) to more complex ones (aeronautical receivers). Thus, spoofing level 1 could be evaluated, as well as the power level required to an effective interference.



SPOOFING IN MOBILE PHONES AND AUTOMOTIVE RECEIVERS

Initially, a test was designed with modulated signal (spoofing) to verify the robustness of different kinds of receivers. The experimental setup, as depicted in Fig. 4 (Electronic Warfare Laboratory of the Technological Institute of Aeronautics – LAB-GE), consisted of the following equipment:

- Modulated Signal Generator Keysight N7609B;
- DHR antenna 0118;
- SMA coaxial cable;
- Software N7609B, for GNSS signals;
- Pedestal for placing the receivers; and
- Semi-anechoic chamber.



Figure 4. Semi-anechoic chamber with the devices under test.

In order to isolate the receivers from any interference or of original GPS satellite signals, the tests were performed in a semi-anechoic chamber. This experiment aimed to test each one of the receivers for their susceptibility to spoofing level 1, radiating the GPS signal generated by the N7609B software. This software allows selecting and simulating signals of GPS and other constellations, such as GLONASS and GALILEO. The power of each one of the satellites can also be controlled, as well as the relative power scale, the pseudo-range, the Doppler shift and the multipath. It is a complex signal generator, allowing different kinds of interaction with GPS receivers and tests. Two programming pages of the software can be seen in Fig. 5.

The experiment was conducted in two phases with increasing level of complexity:

- Modulated signal with false coordinates (static and dynamic) and false date-time data (referring to 2013);
- Modulated signal with false coordinates (static and dynamic) and correct date-time data, consistent with the date of the experiment.

In the first experiment, the automotive receiver was clearly spoofed with a power as low as -50 dBm. The coordinates of Beijing (N40.0096856; W116.478479) were inserted in the receiver, as shown in Fig. 6.

State On State Off Update from Instrument Preset DC Cal Power Search

1. Configuration
Instrument Model Number N5172B/N5182B

2. Basic
Frequency 1.575420000 GHz
Amplitude -50.00 dBm
RF Output On

3. I/Q

4. ALC

5. Baseband

6. AUX IO Global Controls

7. Trigger

8. Real-time AWGN Setup

State On State Off Update from Instrument Preset DC Cal Power Search

Channel	Group	SV ID	Enabled	Frequency	Relative Power Scale (dB)	Power (dBm)	Pseudorange (m)	Pseudorange Error (m)	Doppler Shift (Hz)	Multipath
1	■	G3	✓	L1	0.00	-59.54	21158917.39	0.00	2930.335	0 Taps
2	□	G6	✓	L1	0.00	-59.54	20435999.85	0.00	1394.655	0 Taps
3	□	G13	✓	L1	0.00	-59.54	22042160.43	0.00	2165.636	0 Taps
4	□	G16	✓	L1	0.00	-59.54	20384312.03	0.00	-262.742	0 Taps
5	□	G19	✓	L1	0.00	-59.54	23278140.28	0.00	3804.764	0 Taps
6	□	G21	✓	L1	0.00	-59.54	24949088.41	0.00	958.440	0 Taps
7	□	G23	✓	L1	0.00	-59.54	20918035.95	0.00	111.547	0 Taps
8	□	G30	✓	L1	0.00	-59.54	20844690.72	0.00	-1672.893	0 Taps
9	□	G31	✓	L1	0.00	-59.54	22610579.22	0.00	-2331.388	0 Taps
10	□	E1	□	E1	0.00	-200.00	24971680.47	0.00	2475.513	0 Taps
11	□	E2	□	E1	0.00	-200.00	23446146.07	0.00	246.574	0 Taps
12	□	E3	□	E1	0.00	-200.00	25448254.24	0.00	-2081.097	0 Taps

Figure 5. Programming pages of the N7609B software.



Figure 6. Automotive receiver under static spoofing.

Note that the GPS satellites, designated in the software, were identified (green color) and presented in the receiver (highlighted as 1). Likewise, Beijing coordinates were also presented (highlighted as 2). This spoofing was performed with the insertion of a static coordinate, in which the target was supposed to be stopped at the referred coordinates (highlighted as 3). Thus, the interference (spoofing) was quite efficient, even at extremely low levels of signals (-50 dBm) and the receiver understood that he was in China rather than its actual position in São José dos Campos – São Paulo, Brazil.

In the case of the mobile phone, it was required -30 dBm to spoof the receiver, showing a higher robustness to this action, but remaining already extremely sensitive and vulnerable. In Fig. 7 it is possible to verify the false position of the receiver (highlighted as 1), the coordinates of Beijing (highlighted as 2), and the indication of a static coordinate (highlighted as 3, speed equals to 0).

Subsequently, it has been verified the receivers' susceptibility to spoofing with dynamic coordinates (navigation routes) and false date-time data. Initially it was radiated a power of -50 dBm for both receptors, being gradually increased up to -30 dBm. Then, it was possible to circumvent only the automotive receiver but not the mobile phone.



Figure 7. Mobile phone under static spoofing.

Seeking to increase the complexity and efficiency of the experiment, it was carried on the spoofing with dynamic coordinates, and date-time data compatible with the real ones. Both receivers were corrupted after such a procedure. Figure 8 illustrates it with the closest date-time data (in red arrows), the captured satellites (highlighted as 1), the spoofed coordinates of China (highlighted as 2), the spoofed speed (highlighted as 3) and the present position (highlighted as 4). Both receivers (automotive and mobile phone) could be corrupted with such procedures.

SPOOFING IN AERONAUTICAL RECEIVERS

Similar procedures to the ones previously presented were implemented for aeronautical receivers (GPS stand-alone and EGIR) to evaluate its robustness to spoofing.

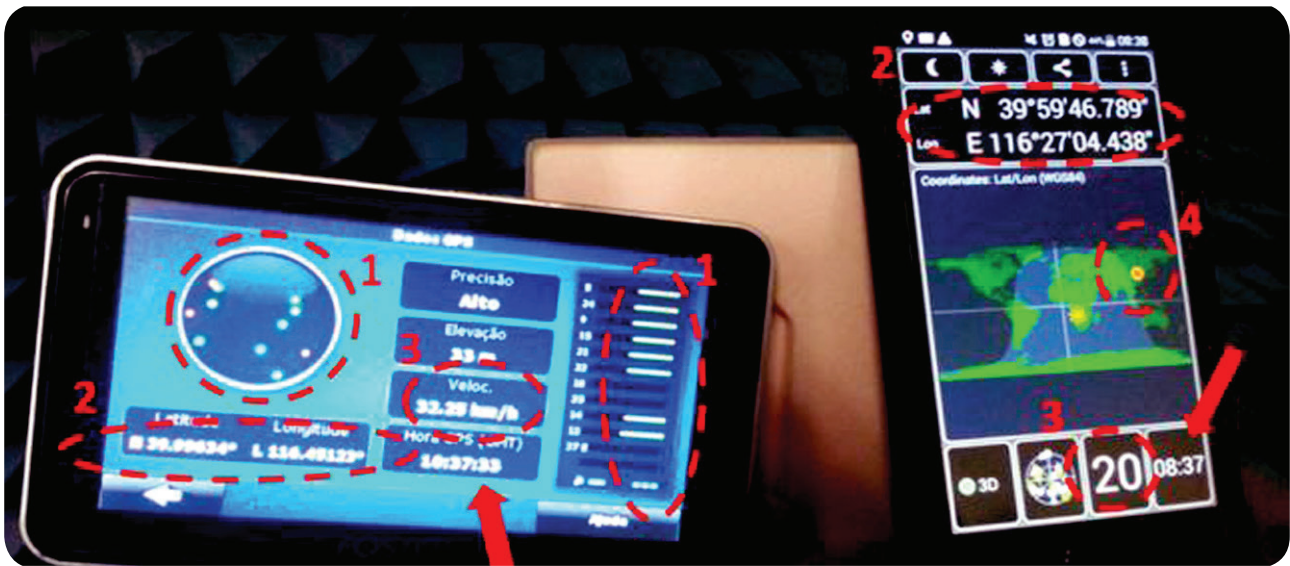


Figure 8. Automotive and mobile phone receivers under dynamic spoofing, with a date-time data close to the real ones.

The aeronautical receiver, known as EGIR, is a solution that assembles a GPS, an Inertial (INS) and a Radio-Altimeter (RALT). It is able to provide three independent solutions:

- INS only;
- GPS only; and
- GPS/INS combined.

In addition, it continuously monitors the performance of each one of the navigation solutions, calculating a Figure of Merit (FOM) associated with the expected error.

After different trials of spoofing in free space, under original and corrupted GPS signals, such receivers have not incorporated the corrupted coordinates. Instead, it presented only a cancelling of the GPS signal, both in GPS stand-alone and in GPS+INS, as seen in Figs. 9 and 10, where, in each figure, the top part indicates the correct coordinates just after the alignment while the bottom part indicates the reading after the spoofing and the loss of the signal. Thus, it acted as a simple jammer, keeping clear the need for further studies on this subject, focusing on the development or implementation of more complex spoofing techniques.



Figure 9. Aeronautical GPS receiver under spoofing.



Figure 10. Aeronautical EGIR receiver under spoofing.

CONCLUSION

As can be seen, GPS devices have been widely disseminated and used in different systems, both for civilian and military applications. However, despite being able to provide great benefits, it should be considered that these systems are, under certain circumstances, vulnerable to intentional interference. Moreover, the deepening dependence of the civil and military infrastructures on GPS and the potential for financial gain or high-profile mischief makes GPS spoofing a gathering threat.

In this work, a series of experiments were carried out, seeking to evaluate the consequences of spoofing to complex systems. The simple experiments that have been developed and described in this work demonstrate that it is straightforward to mount a spoofing attack that could defeat most complex GPS-dependent systems.

Despite this issue is not a widespread concern on internet, and in scientific publications, some conclusions could be drawn from the experiments:

Spoofing level 1 with false date-time data: it was found that the automotive receiver proved to be totally vulnerable. Therefore, less complex spoofed signals, such as the coordinates without the date-time group, were enough to corrupt the coordinates of the equipment under test. However, in more complex receivers, as in the case of mobile phones and aeronautical receivers, it was not possible to corrupt the signal. Based on that, it can be concluded that the interference has been successful for canceling the GPS signal, as a jammer, which eventually can alert the user to the loss of coordinates.

Spoofing level 1 with compliant date-time data: it was possible to verify the success of the interference in the automotive receiver and in mobile phones, which was efficient in static and dynamic scenarios. On the other hand, it was not possible to achieve success in aeronautical receivers (GPS stand-alone and EGIR).

Finally, it was possible to infer the existence of different levels of susceptibility to intentional interference in complex GPS receivers. These results lead to the need of an evaluation of the vulnerability and to the sensibility to spoofing of different equipment and systems, in order to provide adequate countermeasures or, at least, identifying the interference. In addition, it shows the importance of the research and suggests its continuity as an alert to authorities, considering possible problems with adverse groups. Thus, it must be emphasized the strategic importance of this study and showed the profound impact that it can have on social and operational issues.

Moreover, based on recent news on internet, it appears that no sort of encrypted signals or authentication can assure systems against sophisticated spoofing attack, presenting high levels of dangerousness for all systems that use any kind of GPS signals.

AUTHOR'S CONTRIBUTION

Conceptualization, Faria LA and Correia MAF; Methodology, Correia MAF; Investigation, Faria LA; Silvestre CAM and Correia MAF; Writing – Original Draft, Faria LA; Roso NA and Silvestre CAM; Writing – Review & Editing, Faria LA, Roso NA and Silvestre CAM; Resources, Faria LA; Silvestre CAM and Correia MAF; Supervision, Faria LA.

REFERENCES

- Bakker PF (2006) Effects of radio frequency interference on GNSS receiver output. Stevinweg: Delft University of Technology.
- Balvedi GC (2006) Efeitos dos dutos troposféricos na propagação e recepção de sinais GPS (MSc dissertation). São José dos Campos: Aeronautical Institute of Technology. In Portuguese.
- Cavaleri A, Motella B, Pini M, Fantino M (2010) Detection of spoofed GPS signals at code and carrier tracking level. Proceedings of the 5th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (Navitec). doi: 10.1109/navitec.2010.5708016
- Faria LA, Silvestre CAM, Correia MAF (2016) GPS-dependent systems: Vulnerabilities to electromagnetic attacks. Journal of Aerospace Technology and Management 8(4):423-430. doi: 10.5028/jatm.v8i4.632
- Humphreys TE, Ledvina BM, Psiaki ML, O'Hanlon BW, Kintner PM (2008) Assessing the spoofing threat: Development of a portable GPS civilian spoofer. Proceedings of the ION GNSS International Technical Meeting of the Satellite Division; Savannah, USA.
- John A. Volpe National Transportation Systems Center (2001) Vulnerability assessment of the transportation infrastructure relying on the global positioning system.
- Kaplan E, Hegarty C (2006) Understanding GPS: principles and applications. Norwood: Artech House.
- Kuhn MG (2004) An asymmetric security mechanism for navigation signals. Proceedings of the Information Hiding Workshop.
- Ledvina BM, Bencze WJ, Galusha B, Miller I (2010). An in-line anti-spoofing device for legacy civil GPS receivers. Proceedings of the ION International Technical Meeting.
- Motella B, Pini M, Fantino M, Mussalano P, Nicola M, Fortuny-Guasch J, Wildemeersch M, Symeonidis D (2010) Performance assessment of low cost GPS receivers under civilian spoofing attacks. Proceedings of the 5th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (Navitec). doi: 10.1109/navitec.2010.5708018
- Montgomery, PY, Humphreys TE, Ledvina BM (2009) Receiver-autonomous spoofing detection: Experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer. Proceedings of the ION International Technical Meeting.
- Petersomn S (2011) Iran hacked RQ-170 GPS – fooled in autopilot landing in Iran; [accessed 2014 Sep 17]. www.uasvision.com/2011/12/16/iran-hack-rq-170-gps-fooled-in-autopilot-landing-in-iran/
- Papadimitratos P, Jovanovic A (2008a) GNSS-based positioning: Attacks and countermeasures. Proceedings of the IEEE Military Communications Conference (MILCOM). doi: 10.1109/milcom.2008.4753512
- Papadimitratos P, Jovanovic A (2008b) Protection and fundamental vulnerability of GNSS. Proceedings of the International Workshop on Satellite and Space Communications. doi: 10.1109/iwssc.2008.4656777
- Russon MA (2015) Wondering how to hack a military drone? It's all on Google; [accessed 2016 Nov 04]. <http://www.ibtimes.co.uk/wondering-how-hack-military-drone-its-all-google-1500326>
- Tippenhauer NO, Pöpper C, Rasmussen KB, Capkun S (2011) On the requirements for successful GPS spoofing attacks; [accessed 2016 Oct 15] <https://www.cs.ox.ac.uk/files/6489/gps.pdf>
- Warner J, Johnston R (2002) A simple demonstration that the global positioning system (GPS) is vulnerable to spoofing. Journal of Security Administration 25:19-28.
- Warner JS, Johnston, RG (2003) GPS spoofing countermeasures. Homeland Security Journal.