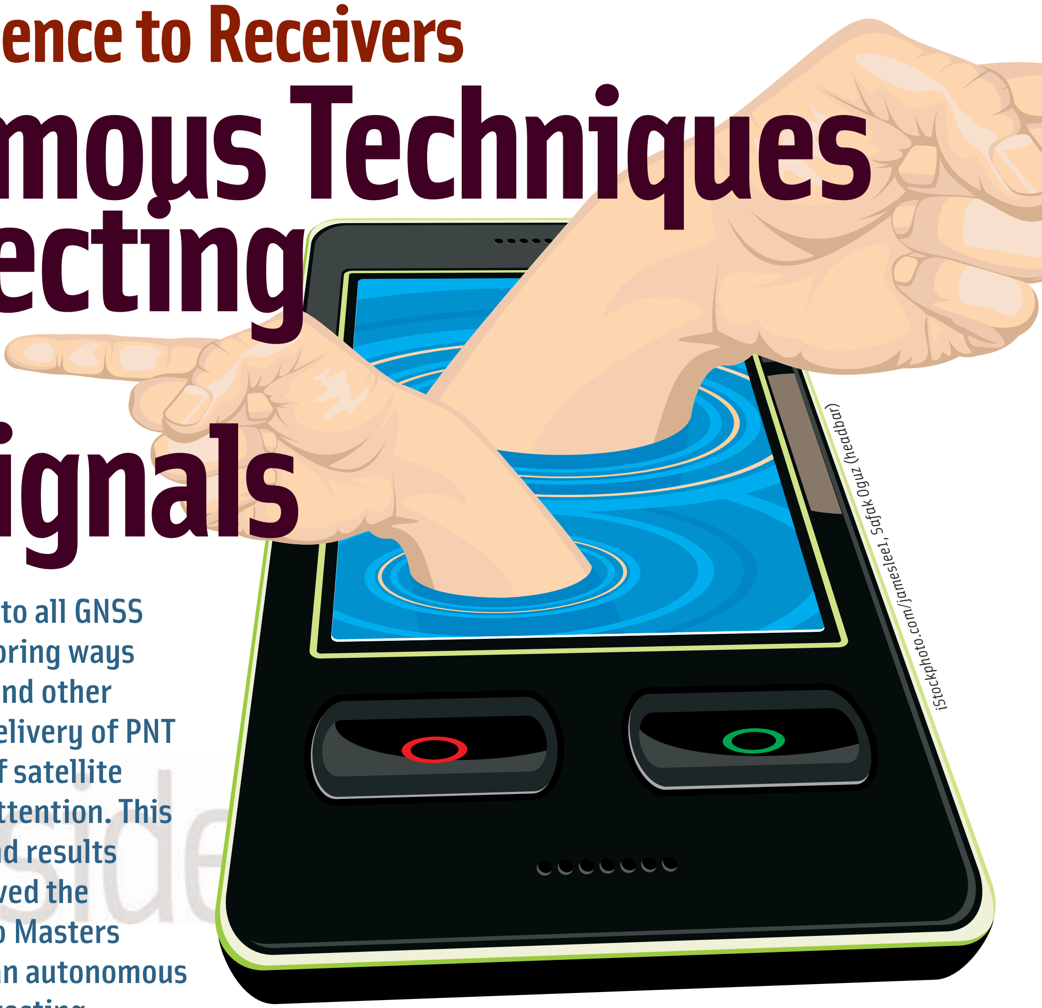
Adding Intelligence to Receivers

Autonomous Techniques for Detecting Flawed GNSS Signals



iStockphoto.com/jameslee1, Safak Oguz (headbar)

In an era of increasing threats to all GNSS systems, researchers are exploring ways to detect jamming, spoofing, and other attempts to prevent reliable delivery of PNT information. Authentication of satellite signals is drawing particular attention. This article describes the design and results of SARA, a proposal that received the DLR special prize of the Galileo Masters competition in 2011. SARA is an autonomous receiver-based method for detecting efforts to interfere with GNSS signals, by first characterizing the behavior of user equipment experiencing various kinds of malicious attacks and then detecting these in real time by comparing those observables with normal receiver operation.

ANTONIO PUJANTE CUADRUPANI
PANAMNAV

GNSS receivers and users, along with the critical infrastructures and services they support, face a growing threat from jamming, spoofing, and meaconing (JSM) events.

Several proposals for GNSS spoofing detection and signal authentication have been proposed over in recent years. These have focused mainly on adding cryptography elements to the GNSS signals and detecting RF characteristics of undesired signals.

The cryptographic approach, for example, lies behind the Selective Availability Anti-Spoofing Module (SAASM) developed by the U.S. Department of Defense. But SAASM-enabled modules cannot be widely applied in civilian applications, but rather are limited to protecting military users and critical civil infrastructures that rely on GNSS signals.

GNSS-based services ranging from synchronization of networks to location-based services are hosted on different kinds of devices. Present-day GNSS receivers are designed as finite state machines (FSM), focused on data presented at an instant in time and integrated through filtering, typically, Kalman filtering, within a narrow time window.

However, the core functionality of GNSS chips is built today with powerful processors that are capable of turning these devices into Turing machines, that is, a descendant of the theoretical computing machine proposed by Alan Turing. This transformation goes beyond a simple FSM by providing decision and analytical capabilities on the information presented to the machine in a larger time window. As it will be shown later, keeping track of data received in a 10 to 30 seconds window is enough to exploit a valuable information to detect and to react to different JSM events.

GNSS chips could incorporate and exploit environmental information by the simple application of Turing principles described in his article, "Computing Machinery and Intelligence," cited in the

Additional Resources section near the end of this article.

The basic concept of Turing machines is to introduce decision algorithm capabilities based on a machine that can read, store, retrieve and analyze data for decision-making purposes and not merely predictably react to present input as is the case with an FSM, one instance of them being present-day GNSS receivers. Turing principles can be synthesized in two aspects: decision-making capabilities and awareness of environmental information.

A particular excerpt of Alan Turing's article seems to be adequate to illustrate our approach to cope with diversity of situations:

> "The displacement of a single electron by a billionth of a centimetre at one moment might make the difference between a man being killed by an avalanche a year later, or escaping. It is an essential property of the mechanical systems which we have called 'discrete-state machines' that this phenomenon does not occur. Even when we consider the actual physical machines instead of the idealised machines, reasonably accurate knowledge of the state at one moment yields reasonably accurate knowledge any number of steps later. As we have mentioned, digital computers fall within the class of discrete- state machines. But the number of states of which such a machine is capable is usually enormously large."

The need for this evolution from FSM to Turing machines arises from the increasing environmental threats to reception of civil GNSS signals. These signals were originally optimized for a JSM-free environment. The evolving operational environment requires a realistic approach to detecting, preventing, and/or mitigating such threats. In this article, we will use the term "malwarnal" — as a conflation of the terms "malware" and "signal" — to refer to intentional JSM events, which are a combination of malicious software applied to generate fake signals.

This article will describe the results of using a new method — SARA (Signal Analysis through Receiver Autonomous techniques) — designed to protect GNSS-based services against JSM events. SARA relies only on information available at the GNSS receiver and does not count on any aid from external sources to distinguish malwarnal from true signals.

The discussion here will reveal the convenience of delivering these observables as standard information for all GNSS receivers, leading to recommendations for manufacturers and standardization initiatives. In this process, a key step involves adequately characterizing the behavior of receiver observables under various signal conditions and distinguishing these behaviors arising from different types of environments.

Exploiting Observables to Characterize and Detect JSM

Several proposals for GNSS signal authentication and malwarnal detection methods have been proposed in recent years. See, for example, the articles by L. Scott, P. Montgomery *et alia,* and T. E. Humphreys and K. Wesson, cited in the Additional Resources section near the end of this article.

These proposals have focused mainly on adding cryptography elements to the GNSS signals and detecting RF characteristics of undesired signals. The SARA proposal aims to be universal by being applicable to any GNSS system (GPS, Galileo, GLONASS, and so on) and at any location on Earth.

For that purpose the guidelines we established for the design of SARA are:

1. autonomy, with the only link to the external world being locally available data (GNSS received signals, inertial measurement units, other signals of opportunity used by the equipment, and so forth)
2. feasibility within current technology boundaries and commercial receiver capabilities
3. unobtrusiveness, not imposing any requirements on GNSS system operators.

These requirements can support a realistic, practical approach based on the signal observables available to existing commercial receivers. This approach leads to a series of recommendations for GNSS receiver design, discussed at the end of this article.

Observables	Receivers		
	1	2	3
Signal/Noise Ratio	Y	Y	Y
Automatic Gain Control		Y	
Position	Y	Y	Y
Signal Lock	Y		
Pseudorange (m)	Y	Y	Y
Doppler deviation (Hz)	Y	Y	Y
Carrier Phase	Y		
Available satellites	Y		
Frame data	Y		

TABLE 1. Observables available for receivers used in tests

We wish to emphasize that SARA is a malwarnal event *detection* technique, not a *mitigation* technique by itself. But SARA provides useful hints on the next step to select the right mitigation technique for each kind of event.

Test Design

Two commercial GNSS simulators provided by DLR, the German Space Agency, have been used for the tests, one configured as the authentic signals source and the other as the spoofer. At the spoofer output, power and signal control devices have been inserted and the line was connected to three commercial GNSS receivers.

Receiver Observables. Each receiver has disparate capabilities, summarized in Table 1.

All receivers generated position updates with a periodicity of one second, which was considered responsive enough for the purpose of malwarnal detection. Discussion will be focused on performance of receiver 1 that delivered the most complete set of data. Receivers 2 and 3 where eventually used to correlate and confirm receiver 1 behavior.

Spoofing Techniques. Two different spoofing techniques have been defined and implemented to test the response of the receivers to malwarnal.

The first technique is well document-

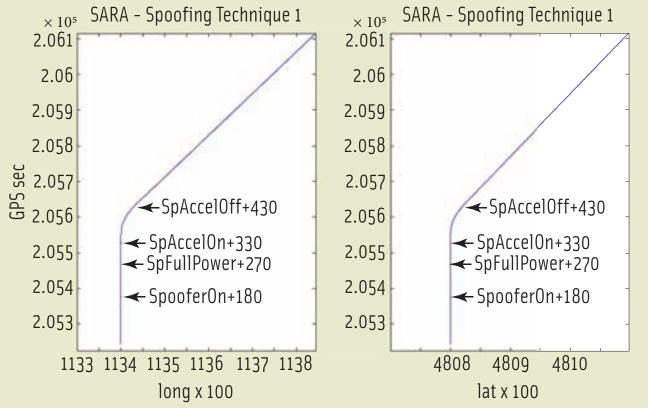


FIGURE 1 Latitude and Longitude deviation induced using Spoofing Technique 1

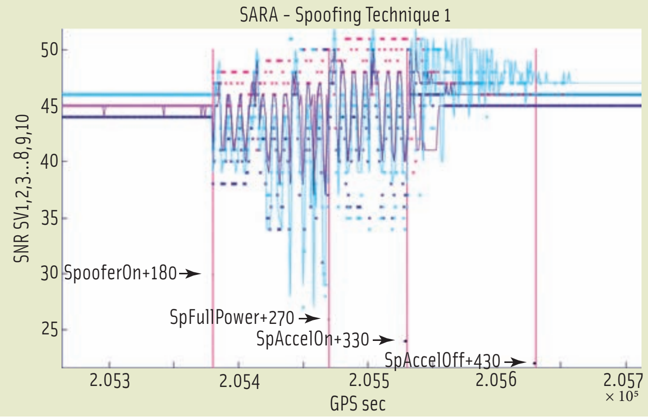


FIGURE 2 Signal-to-noise ratio under spoofing event by PRN, Technique 1

ed in literature and uses live GPS signals in space to first align its correlation peak with that of the target receiver and that gradually transmits counterfeit signals to lead the receiver astray. See the article by T. E. Humphreys *et alia* cited in Additional Resources.

The second spoofing technique uses a different approach, the attributes of which, for reasons of public safety, will only be summarized here along with those of the first technique. (See **Table 2**.)

The following spoofing steps were triggered with respect to start of simulation at GPS second 205200:

1) For technique 1 and 2:
timeSpooferOn = 205200 + 180 seconds, spoofing simulator is switched on
timeSpooferFullPower = 205200 + 270 seconds, spoofing simulator at full power
2) For Technique 1:
timeSpooferAccelOn = 205200 + 330 seconds, spoofing simulator starts course deviation
timeSpooferAccelOff = 205200 + 430 seconds, spoofing simulator sustained new course

The next section presents a detailed discussion of the effect of each spoofing technique upon the behavior of receivers. The response of receivers to changes in signal observables as a result of spoofing can suggest methods for detecting JSM events.

Technique 1: Observables and Receiver Response

Spoofing Technique Attributes	1	2
Difficulty for spoofing a vehicle	High	Low
Difficulty for spoofing a stationary receiver	Low	Low
Time to implement	10 to 30 minutes, slow	2 to 5 minutes, quick
Time to setup	2 hours	1 hour
Meaconing	No	Yes
Detectability if no other local references are available	Low	Low
Detectability, using other local references and observables	High	Possible
Detectability, using non-local references	High	High
Estimated Cost	$40K simulator	$10K simulator/recorder

TABLE 2. Attributes of spoofing techniques

Spoofing Technique 1 was simulated at several different power levels, from 0 to 9 decibels, and inducing a deviation in latitude and longitude at a rate of 15 meters/second and a heading of 45 degrees on a static target, shown in **Figure 1**.

Figures 2 through 8 correspond to a spoofer signal level three decibels stronger than the authentic GPS signals. This power level was chosen to ensure capture of the receiver by the spoofer and allowed us to focus on the behavior of the receiver observables.

Even with a spoofing power level differential between 0 and +1.5 decibels, capture by the spoofing signal is not always certain for all three types of receivers, which is consistent with the findings described in the article by D. Shepard cited in Additional Resources.

To ensure capture of a receiver by the spoofing signal, a minimum of three decibels more power is necessary. Signal-to-noise ratio (SNR) and signal lock appear to be the most responsive observables. They react instantaneously to the different steps of the spoofing attack.

SNR levels show an increase under spoofing conditions and a transitional sinusoidal shape, which can be explained as fluctuations of the carrier tracking loop as it switches back and forth between the desired or authentic GPS signals and the spoofing signals, as illustrated in **Figure 2** (The desired signal is present throughout the simulation.)

Signal lock is lost at the beginning of the spoofing event, showing high sensitivity to power capture and change-of-course phases. (See **Figure 3**.)

Pseudorange and Doppler readings seem to react to the spoofing with considerable delay; however, under nominal orbit conditions a significant discontinuity in the expected smooth and locally near-linear behavior of these observables appears after spoofing is initiated.

Figure 4 shows the deviations in Doppler frequency of the authentic GPS signals in the presence of spoofing. Due to the associated delay, these observables can be used to obtain further confirmation of the presence of a spoofing attack

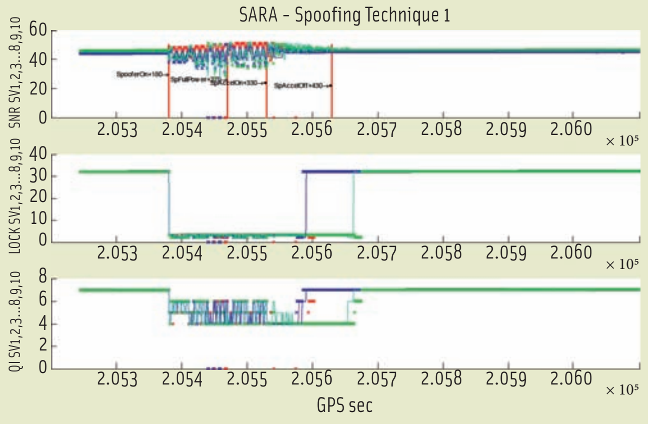


FIGURE 3 SNR and signal lock evolution by PRN, Technique 1

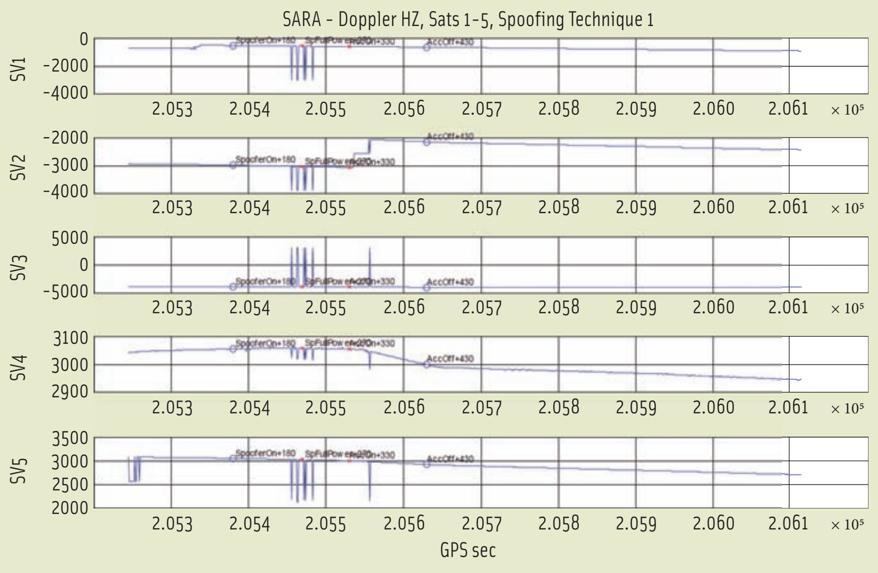


FIGURE 4 Doppler frequency deviation, Technique 1

rather than triggering a warning. This seems to corroborate the prediction of Turing in the excerpt referring to the avalanche effect quoted before.

This is also the behavior of carrier phase readings, as can be seen in Figure 5 with signals identified by pseudorandom noise (PRN) codes, which show a considerable latency in response at the start of power capture and acceleration phases.

NMEA data deserve a particular comment. As reflected in our tests, timing delivered through NMEA messages ($GPZDA, $GPGLL) seem to ignore the presence of the spoofing attack and continue to deliver data. This is particularly relevant considering that most GPS-based applications rely on NMEA messages as a valid input.

This behavior has also been reported in other tests, including those described in the article by D. Shepard *et alia*. This reflects the fact that receiver architecture is designed to use GPS data as a locking reference rather than a real-time source for timing information.

NMEA position data ($GPGLL message) also exhibits a slow response behavior. Spoofer power level differentials above three decibels are necessary to trigger discontinuity in $GPGLL data. Discontinuity then appears during the change-of-course phase.

Receivers lock to spoofing signals with fidelity. This is, on the other hand, a proof that receiver designs show a remarkably robust tracking behavior for GNSS users when operating in ideal environments without malwarnal. Figure 6 displays a $GPGLL disruption with a four decibel higher spoofer signal power.

Frame data from navigation messages and the number of satellites delivering reliable data also have been shown to be highly responsive observables and provide a good metric not only to detect but also to characterize different JSM events. This can be observed in Figure 7 and Figure 8, which show the dramatic struggle for receiver capture by the spoofing signal. When the number of satellites providing frame data recovers, as shown in Figure 7, the spoofing PRN signals have supplanted the authentic ones, in what could be called a "cuckoo" effect.

For test purposes, a particular sequence containing the term 'fool' in

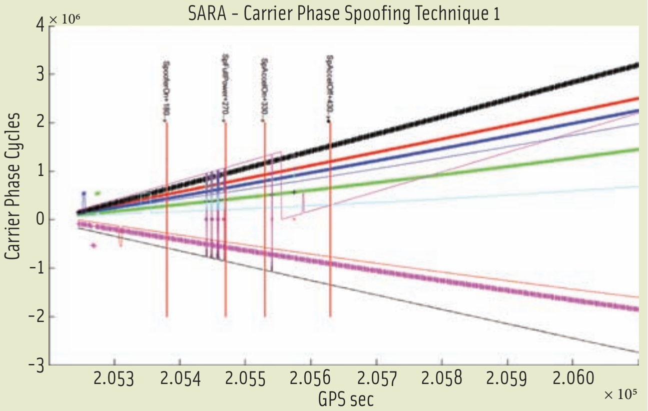


FIGURE 5 Carrier phase evolution by PRN code, Technique 1

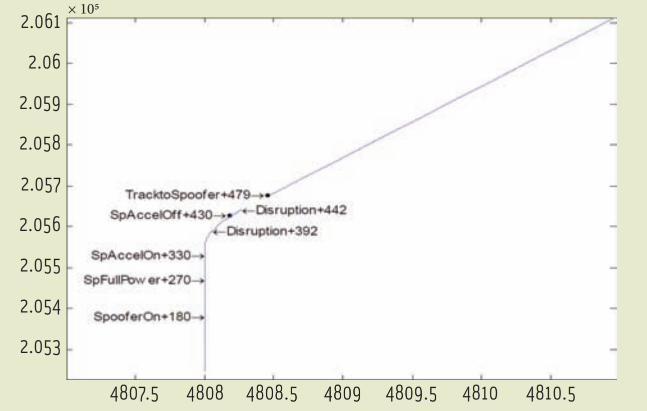


FIGURE 6 $GPGLL disruption with 4dB higher spoofer power, Technique 1

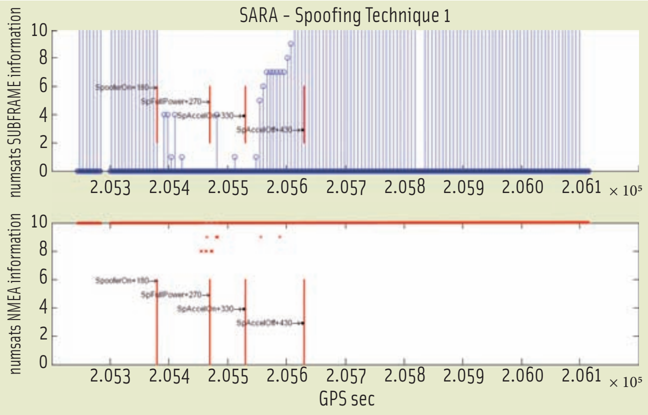


FIGURE 7 Number of PRNs providing NMEA data and frame data during spoofing event, Technique 1

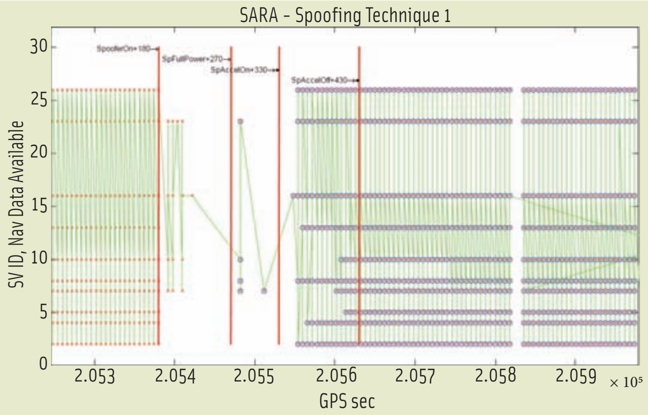


FIGURE 8 Frame data evolution by PRN code during spoofing event, Technique 1

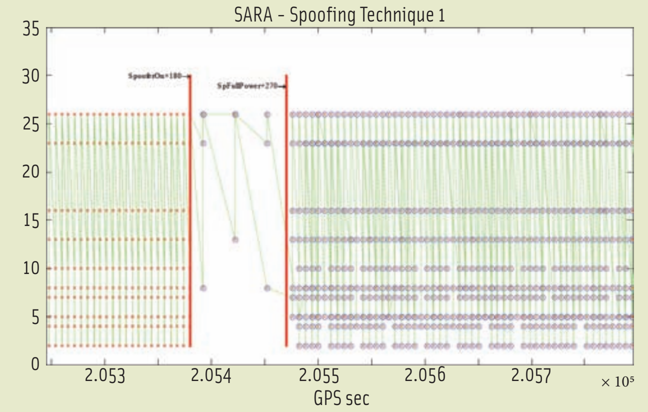


FIGURE 9 Frame data evolution by PRN code during spoofing event, Technique 2

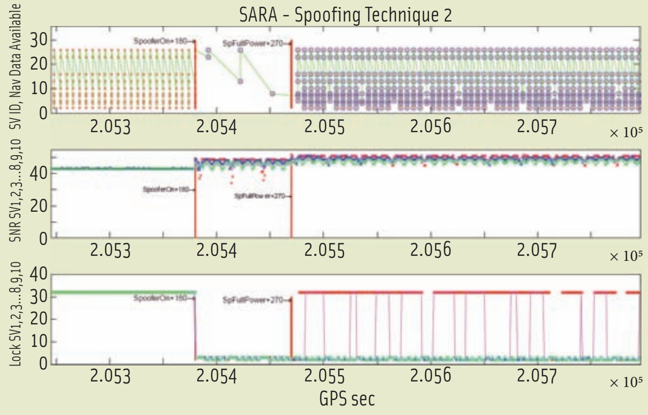


FIGURE 10 Frame data, SNR and signal lock, by PRN, Technique 2

hexadecimal notation to differentiate the spoofing frame was inserted into free bits in the navigation message, represented by blue dots in Figure 8. Bits of word 2 and word 3 in subframe 1 also were modified for identification with the IP address of PanamNav.com in hexadecimal notation to differentiate the tests from intentional spoofing, in an approach inspired by biological techniques as described in the article by H. O. Smith and J. C. Venter. The authentic GPS signal is displayed with red crosses.

Figure 8 reveals the anatomy of the evolution over time of this type of spoofing attack. An analysis of the results from this series of tests leads to the following conclusions: (a) loss of lock and capture are progressive and independent for each PRN code, (b) no correlation exists between the loss of the wanted signal for each PRN code and the instant of capture by the spoofer, and (c) capture is successful only after full power is achieved and a transitory course deviation phase is consolidated.

Technique 2: Observables and Receiver Response Figure 9 shows the profile of the spoofing event for Technique 2. No position drift is introduced in this case and capture requires higher power, because the authentic GPS signals and the spoofing signals are struggling to capture the tracking loop without a noticeable advantage at equal power levels. However, this technique requires less resources and preparation, as shown in Table 2.

Note that (a) lock loss and capture of a signal is quasi-simultaneous for each PRN code, (b) some PRN codes show subframe data discontinuity after capture (which is exploited by SARA algorithms), and (c) capture is successful only after full power is achieved.

Figure 10 shows the correlation between subframe data, SNR, and signal lock. Note that some differences appear among these observables with respect to Technique 1. The SNR increases during the spoofing event and remains stable, without oscillations. Carrier lock is lost during the spoofing event and shows random (non-periodic) oscillations.

Figure 9 showed the relevance of monitoring frame data, because in using Technique 2 other observables — such as NMEA data, Doppler frequency and carrier phase — display no reaction, as can be seen in Figures 11, 12 and 13, respectively.

Receiver Response to Jamming

For comparison with Techniques 1 and 2, a jamming event was generated with a portable jamming device receiving GPS signals-in-space. Figures 14, 15, and 16 show the resulting behavior of, respectively, frame data, SNR, signal lock, and NMEA data.

The effect of the jamming signal is

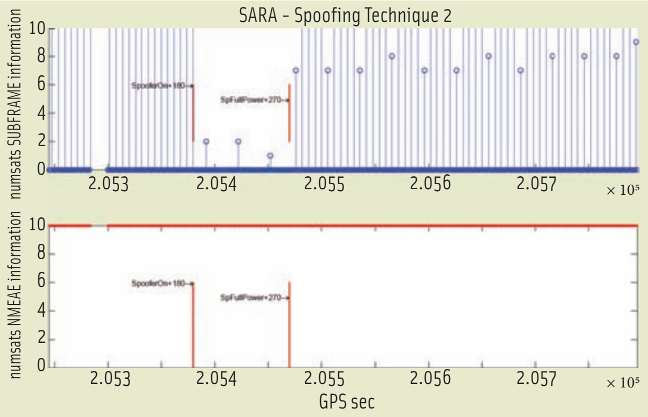


FIGURE 11 Number of PRNs providing NMEA data and frame data during spoofing event, Technique 2

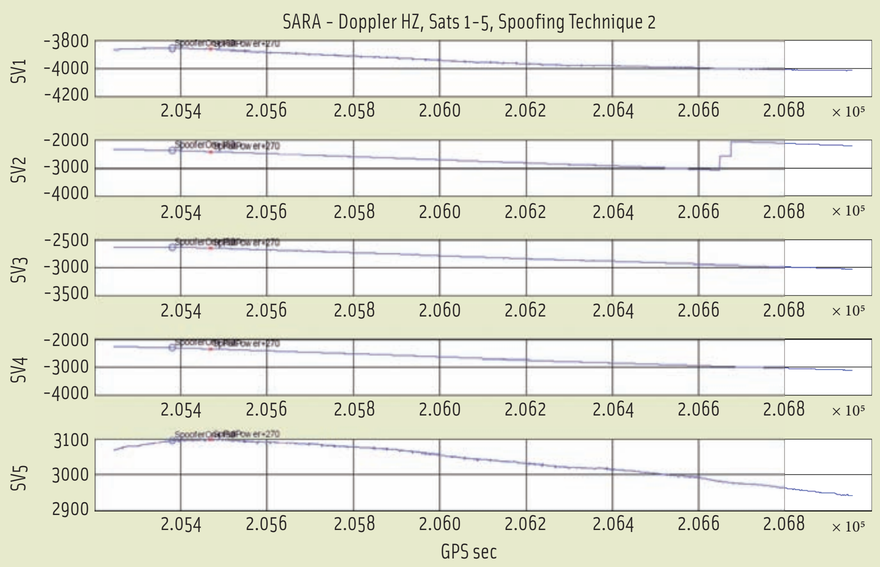


FIGURE 12 Doppler frequency deviation by PRN, Technique 2

definitive and sharp in time, at both the start and end of the event. In this case, a clear correlation between the loss of frame data and loss of NMEA data appears, which was not the case with the spoofing events. SNR and signal lock show also a clear and distinguishable sharp drop.

This distinct reaction is also observed in Doppler deviation and carrier phase (**Figures 17** and **18**), which register sharp peak variations. Carrier phase output is zero during the jamming event period, as expected.

Receiver Response to Loss of Line-of-Sight

We also compared receivers' response to the loss of line-of-sight (LoS) signals with their behavior during jamming and spoofing events. The goal is to characterize the LoS loss profile (e.g., a vehicle in a tunnel or a pedestrian in indoor conditions) in order to avoid false jamming/spoofing alarms. The tests were conducted indoors using recorded signal-in-space data.

For static GNSS receivers (typically used for synchronization purposes) LoS loss of all satellites is an unlikely event. The results for frame data, SNR, signal lock and NMEA data are shown in **Figures 19**, **20** and **21**.

Here the most distinguishable traits are the evolution of the SNR and the availability of NMEA data. These observables reflect clearly the random variable conditions of indoor reception due to variation in signal penetration through windows and different types of building materials.

The frame data shows a behavior very similar to jamming conditions. Consequently, in this case this observable cannot be used as a reference to distinguish from jamming. But both frame data for jamming and LoS loss are clearly distinguishable from spoofing. In jamming and LoS scenarios, frame data by PRN has a sharp fading, while in the spoof-

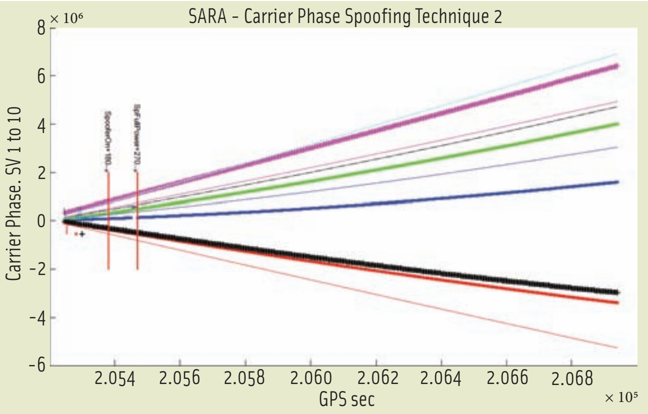


FIGURE 13 Carrier phase evolution by PRN, Technique 2

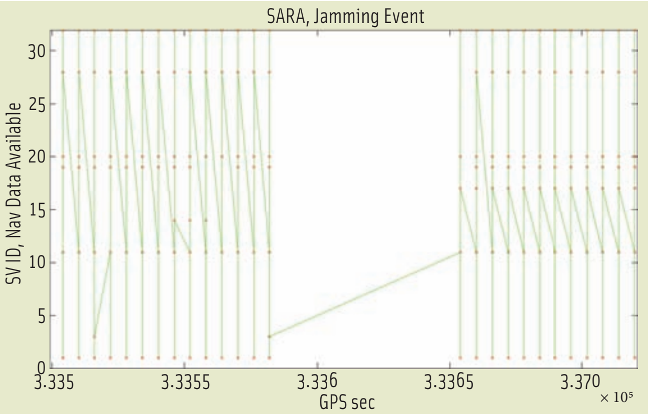


FIGURE 14 Frame data evolution by PRN code during a jamming event.

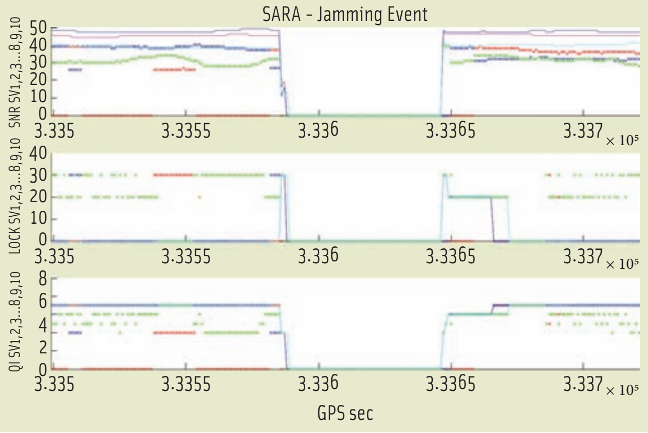


FIGURE 15 SNR and signal lock response during a jamming event.

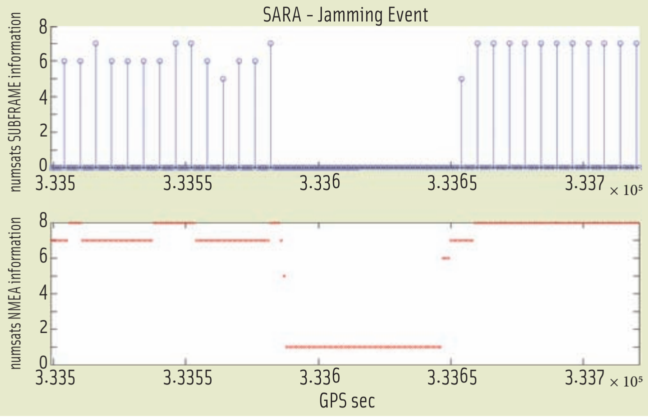


FIGURE 16 Number of PRNs providing NMEA data and frame data during a jamming event

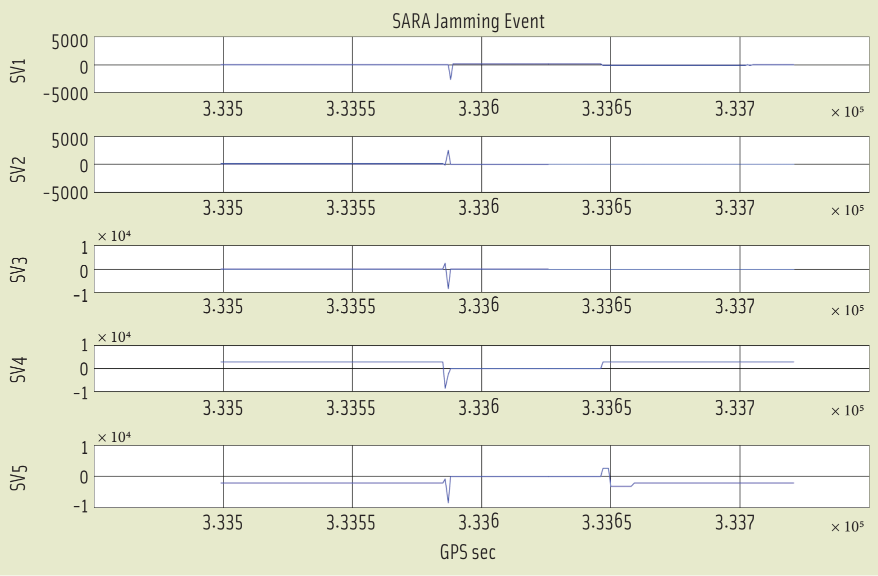


FIGURE 17 Number of PRNs providing NMEA data and frame data during a jamming event

ing event the handover from authentic PRNs to spoofing PRNs is progressive and non-correlated among PRNs.

On the other hand, the observed continuous fluctuations of Doppler and carrier phase readings presented in **Figures 22** and **23** are characteristic of indoor reception, and the behavior is quite different from jamming but closer to spoofing Technique 1.

Conclusions

Analysis of various receiver observables has been carried out for two spoofing techniques, jamming, and LoS loss events.

Spoofing Technique 2 is the most difficult to detect but is easier and less demanding to implement. (Only jamming is simpler to implement.) Further research is required to better characterize this technique.

Each kind of event has a particular fingerprint of observables. A matrix decision tool could be built on these results to detect JSM events and avoid false alarms.

SARA enables the assessment of the authenticity of received GNSS signals —

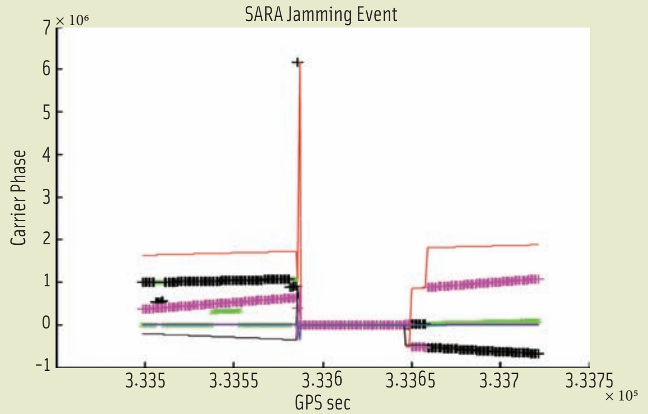


FIGURE 18 Number of PRNs providing NMEA data and frame data during a jamming event

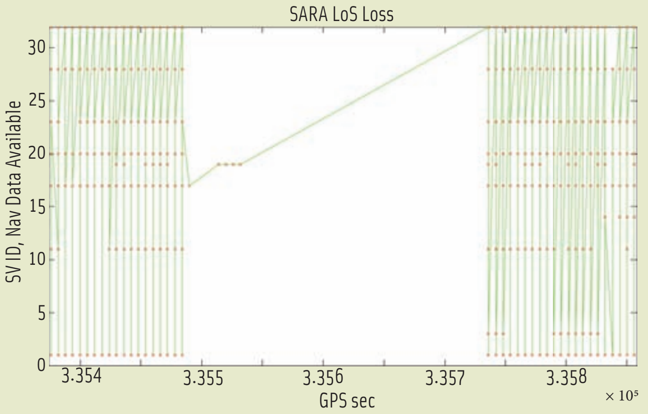


FIGURE 19 Frame data evolution by PRN code during an LoS loss event.

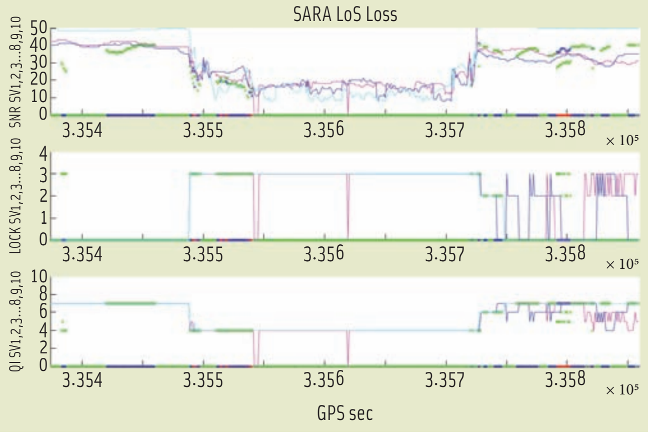


FIGURE 20 SNR and signal lock evolution by PRN during during an LoS loss event

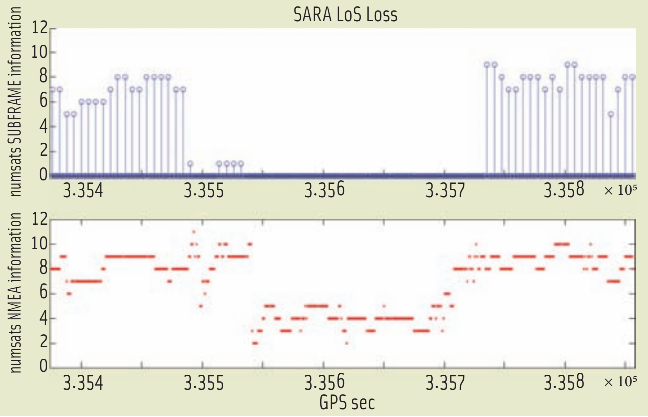


FIGURE 21 Number or PRNs providing NMEA data and frame data during an LoS loss event

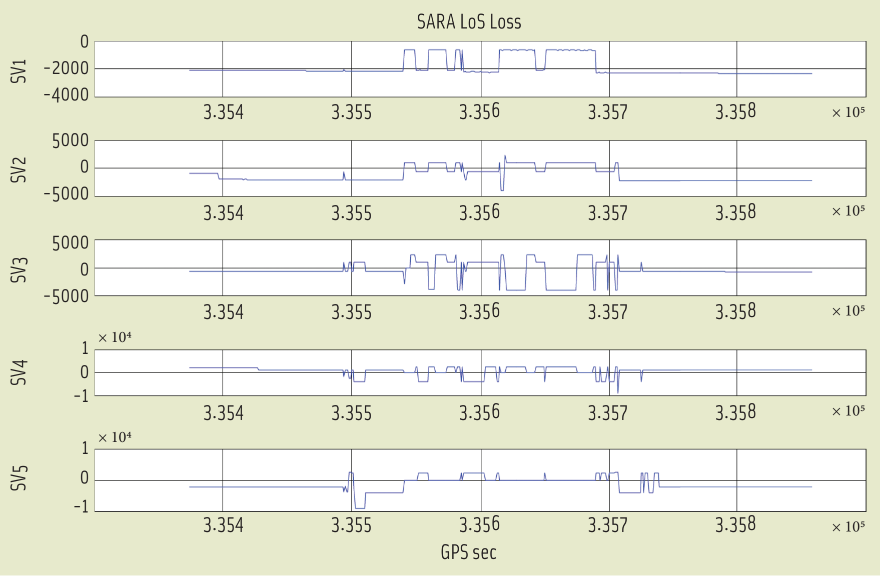


FIGURE 22 Doppler frequency deviation by PRN during a LoS loss event

and the issuance of warnings for false signals, based on continuous monitoring supported by a processor embedded in the receiver.

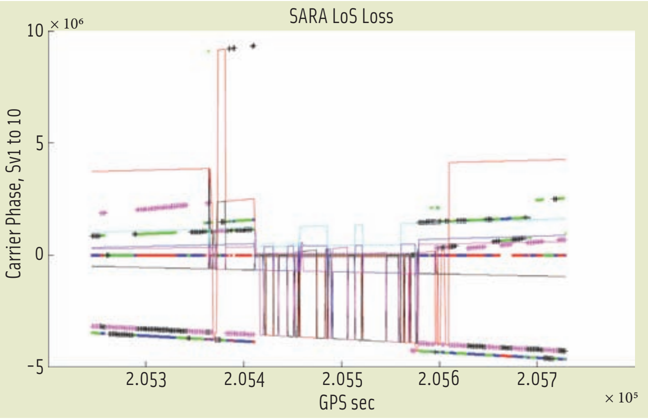


FIGURE 23 Carrier phase evolution by PRN code during an LoS loss event

A possible decision matrix based on four main observables is shown in Table 3.

One key advantage of SARA is its multisystem nature; the concepts are applicable to several GNSS systems, as long as the receivers can process the various signals and provide the necessary information on the behavior of observables.

SARA also avoids the narrowing of receiver performance in fighting JSM events. The navigation and timing solutions of GPS receivers meant to operate under a wide variety of signal dynamics could be widely manipulated by a spoofer. With SARA techniques, observing and tracking the signal behavior allows for a wide range of receiver design and dynamics to enable them to track and follow GNSS signals without giving up agile performance.

As might be expected, SARA can be a helpful complement for receiver autonomous integrity monitoring (RAIM) techniques. RAIM aims at identifying unintentional system impairments in GNSS satellites that may lead to wrong PNT solutions.

However, RAIM is not designed to detect false signals in all PRN codes simultaneously and, thus, is vulnerable to spoofing. SARA, on the other hand, simultaneously gathers and records the evolution of all received signal sources, detecting not only spoofing but also other possible events and system outages.

The discussion in this article has shown that the provision of adequate observables makes it possible to turn GNSS receivers into Turing machines — in other words, to be able to incorporate algorithms for the active monitoring of signal behavior to detect JSM events and reject non-authentic signals in real time.

From this study, we can recommend several possible actions for standardization and design of GNSS receivers in order to cope with an increasingly challenging signal environment in which malwarnal will be ever more common in the near future:

Observable	Type of event			
	T1	T2	Jamming	LoS loss
SNR	Oscillations, SNR increase	No oscillation, SNR increase	Sharp drop at event edges	Random drop between event edges
Doppler	Late spikes	No reaction	Spike at event edge	Random drop between event edges
Carrier Phase	Late spikes	No reaction	Spike at event edge, zero on event	Random drop between event edges
Frame Data	Progressive, no correlation with PRN code	Sharp, some PRN code missing data	Sharp at event edge	Sharp at event edge

TABLE 3. Event profile versus observables

1. Provide observables beyond presently standardized NMEA data. These would include some of the observables used in this study, such as Doppler deviation readings, correlated SNR and signal lock, carrier phase, PRNs for which receiver delivers NMEA data, PRNs for which receiver delivers frame data, and frame data evolution and characteristics.
2. Provide paired automatic gain control (AGC) and SNR information. Unfortunately, AGC information was not available in all receivers during this study. It would be useful to cross-correlate SNR and AGC data to help detect and differentiate JSM events from indoor conditions.
3. Provide actual bits readings from navigation messages frame data. This would allow for further signal health and reliability check in real time.

SARA techniques can be complemented by local predictions and observables from external sources, such as a reference signal-monitoring center. PanamNav is developing these techniques using the framework of the TIMEWISE project that was awarded the Gate Galileo Masters Special prize 2011<http://www.galileo-masters.eu/index.php?anzeige=gate11.html> . Further results will be offered in future publications.

The concepts and methods presented in the present paper are covered by a patent application filed by the author.

Acknowledgments

The author wishes to acknowledge Dr. Leandro de Haro, Dr. Miguel Calvo, Dr. Ramón Martinez, Luis Cuellar, and David Marcos from the Radio Signals Group of Universidad Politécnica de Madrid for the implementation of the hardware developments for the tests; Dr. R. Agraz del Alamo, Pablo Pisonero, Daniel Chung, and Alberto Baeza from PanamNav for the comments on the paper; Dr. Rolf-Dieter Fischer, Dr. Michael Meurer, Robert Klarner, Dr. Achim Hornbostel, Dr. Andriy Konovaltsev, and Christian Haettich for their support and implementation of the simulation test bed in the framework of the DLR (Deutschen Zentrums für Luft- und Raumfahrt) Galileo Masters Special prize 2011.

Manufacturer

The DLR simulators were from **Spirent Communications,** Paignton, Devon, United Kingdom.

Additional Resources

[1] Galileo Masters Awards 2011, <http://www.galileo-masters.eu/index.php?anzeige=winner2011.html>

[2] Humphreys, T. E., and B. Ledvina and M. Psiaki, "Assessing the Spoofing Threat: Development of a Portable GPS civilian Spoofer," in *Proceedings of the ION GNSS Conference,* Portland, Oregon USA, September 2008

[3] Humphreys, T. E., and K. Wesson, "Detection Strategy for Cryptographic Civil GNSS Anti-Spoofing," *IEEE Transactions on Aerospace and Electronic Systems,* 2012

[4] Montgomery, P. Y., and T. E. Humphreys, and B. M. Ledvina, "Receiver-Autonomous Spoofing Detection: Experimental Results of a Multi-Antenna Receiver Defense against a Portable Civil GPS Spoofer," *Proceedings of the 2009 International Technical Meeting of The Institute of Navigation,* January 2009

[5] Shepard, D., "Characterization of Receiver Response to Spoofing Attacks", Bachelor's degree thesis, Presented to the Faculty of the Undergraduate School of The University of Texas at Austin, May 2011

[6] Shepard, D. P., and T. E. Humphreys and A. A. Fansler, "Going Up Against Time", *GPS World,* August 2012

[7] Smith, H. O., and J. C. Venter, "Creation of a Bacterial Cell Controlled by a Chemically Synthesized Genome," *Science* Vol. 329 no. 5987 pp. 52-56, July 2, 2010

[8] Turing, A.M. (1950). Computing machinery and intelligence. Mind, 59, 433-460

[9] Scott, L., "Anti-Spoofing & Authenticated Signal Architectures for Civil Navigation Systems," ION GPS/GNSS 2003, Portland, Oregon, September 2003

[10] "Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System," Technical Report, John A. Volpe National Transportation Systems Center, August 29, 2001

Author

Antonio Pujante Cuadrupani is responsible for the PanamNav project, a world reference in GNSS authentication solutions. He holds a Ph.D. and a M.Sc. in engineering from Universidad Politécnica de Madrid. He has been awarded two Galileo Masters Special Prizes (DLR and Gate/NavCert/IFEN) from the European Satellite Navigation Competition (ESNC) for his work on GNSS authentication. He was also a finalist in 2011 in North America and Bavaria regional competitions and first runner-up in 2012 in the Prague regional contest of the ESNC. PanamNav has also received in 2012 the IBM SmartCamp prize, the CeBit innovation prize, the StartEurope innovation prize and in 2013 the Wayra/Telefónica prize. Pujante has worked for Hispasat (1991–1994), Telefónica Sistemas (1994–1997), Eutelsat (1997–2005) and the European Space Agency (2005–2010). He has participated in the design and implementation of more than 25 satellites for Eutelsat and Hispasat and has been contributor to the development of the DVB-S, DVB-S2 and DVB-RCS standards. At ESA Pujante served as an officer for several activities related to advanced technology and GNSS studies. He has more than 20 international publications in satellite communications and GNSS and holds three patents on GNSS and communications.