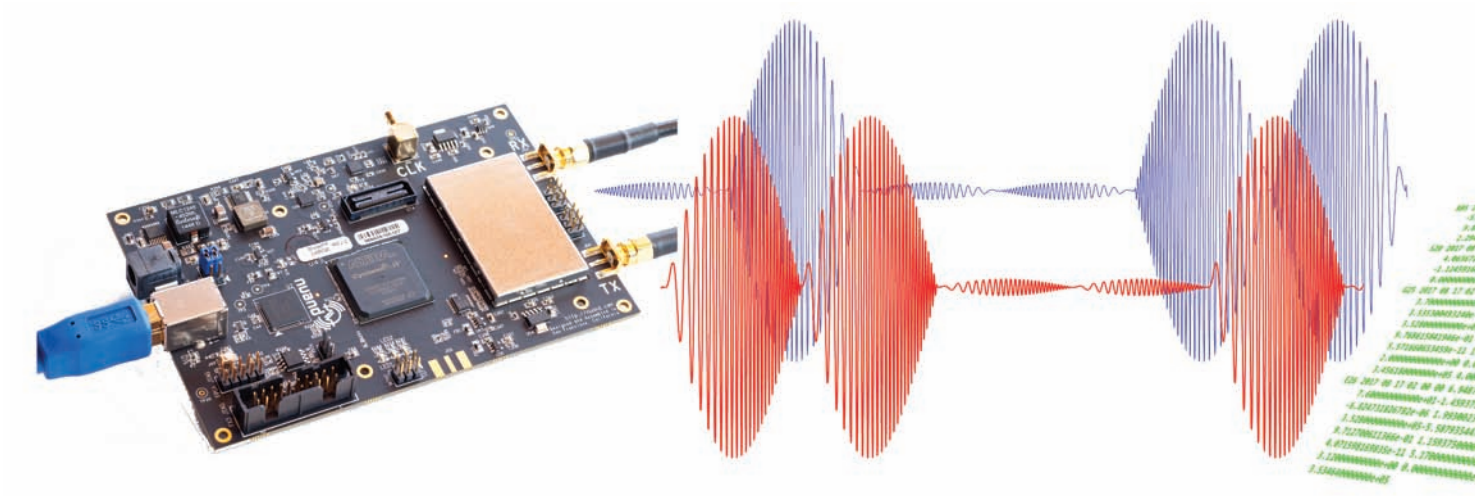
A Look at the Threat of **Systematic Jamming of GNSS**



Research to date has considered two extremes of interference: simple jamming sources that aim to overpower GNSS signals; and sophisticated spoofing signals that aim to covertly mislead GNSS receivers. However, there appears to be a middle-ground between jamming and spoofing that might thwart current detection, localization and mitigation techniques. In terms of technology and cost, it appears to be very accessible to a malicious attacker. This article represents only a very preliminary examination of the concept on mitigating the threat of systemic jamming of GNSS, but does seem to highlight the fact that it may be naïve to assume that the jamming threat will not evolve in reaction to anti-jamming technology. The notion that jamming devices might be designed in direct response to anti-jamming techniques might open a new avenue of research into the more game-theoretic aspects of resilient GNSS receivers. It might further invigorate the use of technologies like antenna diversity, or synthetic aperture antennas, or adaptive interference mitigation techniques.

JAMES T. CURRAN
INDEPENDENT RESEARCHER, CORK, IRELAND

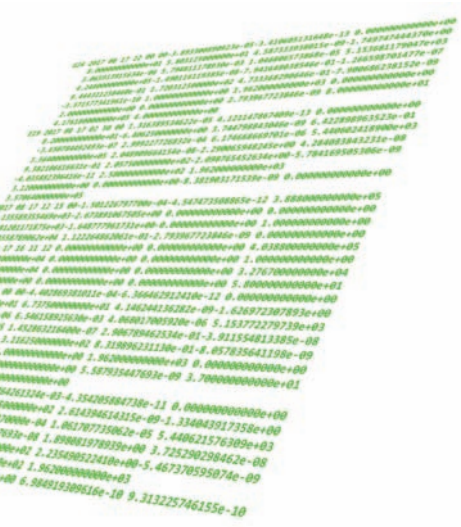
MICHELE BAVARO
EUROPEAN COMMISSION, JOINT RESEARCH CENTRE, ISPRA, ITALY

PAU CLOSAS
NORTHEASTERN UNIVERSITY, BOSTON, MA, USA

MONICA NAVARRO
CENTRE TECNOLÓGIC TELECOMUNICACIONS CATALUNYA, BARCELONA, SPAIN

The vulnerability of GNSS to various forms of malicious interference have been widely discussed in recent years, and have considered a wide range of both real and potential attacks. Some of these have included extensive studies of commercially available jamming devices, while others have considered the more comprehensive case of spoofing, where the interference takes the form of genuine GNSS signals (For details, see papers listed in Additional Resources, including M. G. Amin *et alia*).

Studies of simple jamming attacks have demonstrated that it is relatively easy, given sufficient broadcast power, to deny the use of GNSS to many commercial receivers (For details, see papers listed in Additional Resources, including M. Johnson and R. Erlandson). However, it has also been shown that given the easily identifiable or periodic nature of simple jamming signals, a receiver can often mitigate the threat, for example, via the use of adaptive filtering or pulse blanking (F. Dovis, Additional Resources). Furthermore, it has been demonstrated that the jamming signal itself can be readily exploited to identify and locate the jamming source. On the other



hand, recent work on GNSS spoofing has shown that current receivers are vulnerable to a well calibrated spoofing attack (T. E. Humphreys, *et alia*), and it is clear that many receivers can be manipulated without arousing any suspicion. However, such attacks are highly complicated and require knowledge of the GNSS signals, and the attack scenario, including precise timing and positioning.

It is highlighted here that a middle ground exists between the simple jammer and the spoofer, and it is the most likely "next step" for the malicious adversary. A typical jammer is blind to the GNSS signals it overwhelms, and simply relies on power and spectral occupation to deny the GNSS signals. In contrast, a spoofing device must faithfully replicate the characteristics of genuine GNSS signals. As such, spoofing is highly sensitive to alignment of time, phase and power of the spoofing signals with respect to the genuine signals. It is suggested that it is possible to create a device, only slightly more complex than a simple jammer, that can increase the efficiency of a jamming-based denial-of-service (DOS) attack.

Specifically, this work introduces the concept of systematic jamming: where a simple jammer might be combined with information of the GNSS signals to produce a more sophisticated jamming signal. For example, a jammer may be equipped with a simple low-cost commercial GNSS receiver, providing accurate position, time and satellite ephemerides. With this information, it might be possible to trigger short and sparse bursts of interference, such as to deny GNSS to a nearby receiver with a very low average power. In this manner, a receiver might be unable to: reliably detect that a jamming attack was ongoing; to effectively mitigate the jamming attack; or to identify or localize the jamming source. In the work that follows, we consider what form such a jammer might take, what the implications for the nearby target receiver might be, and how a target receiver might be equipped to thwart such an attack.

The basic principle is that for standalone GNSS, the position, velocity and time (PVT) can be denied by either: denying the physical layer, on which the ranging measurements are made; or by denying the data layer, prohibiting the recovery of ephemeris or transmit time; or both. Because the data layer need only be sporadically interrupted to completely deny the message recovery, it represents the weakest link in the PVT generation. It is therefore the obvious target, particularly when channel coding is not present in the jammed signal.

Problem Definition

This work considers the threat that might be posed if a malicious adversary were to add a small amount of added complexity to the typical GNSS jammer, with the intention of providing bursts of interference at specific epochs. A modification to the typical GNSS jammer is envisaged, which includes an on/off keying driven by a micro-controller, as depicted in **Figure 1**. The algorithm controlling the keying employs position and timing information sourced from a simple, low-cost GNSS consumer-grade receiver (naturally, care must be taken to avoid self-interference). Using the GNSS measurements, accurate estimates of the transmit-time observed on GNSS signals seen in the vicinity of the jammer can be computed.

It is proposed that this information might be exploited by an adversary to trigger short pulses of interference which are tightly aligned with specific portions of the navigation message of each satellite. Previous work has demonstrated that a low duty-cycle pulsed interference, appropriately synchronized with the navigation message, can cause disruption to the receiver data recovery process, equivalent to that of an always-on interference (J. Curran *et alia,* Additional Resources). This process requires that the pulse pattern be designed to specifically target weaknesses in the navigation message coding scheme, and it has been shown that a malicious adversary might inflict a DOS upon a naïve receiver, using an average interference power 10 to 20 decibels lower than continuous interference.

Naturally, this offers some distinct advantages to the adversary: a given broadcast power might impose a DOS over a wider geographical area; by broadcasting short sporadic bursts of interference, it may be more difficult

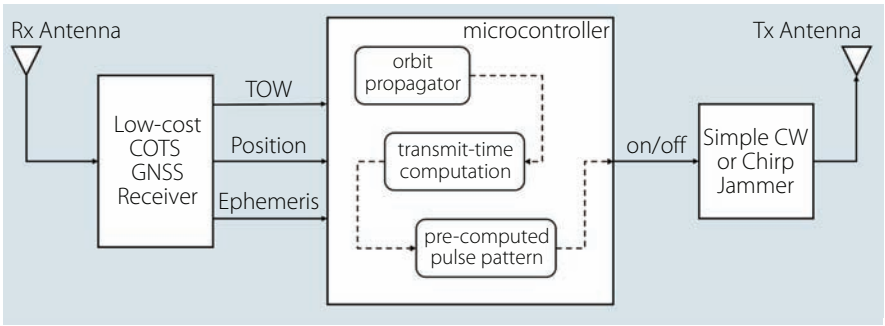


FIGURE 1 A block diagram of a hypothetical systematic jammer

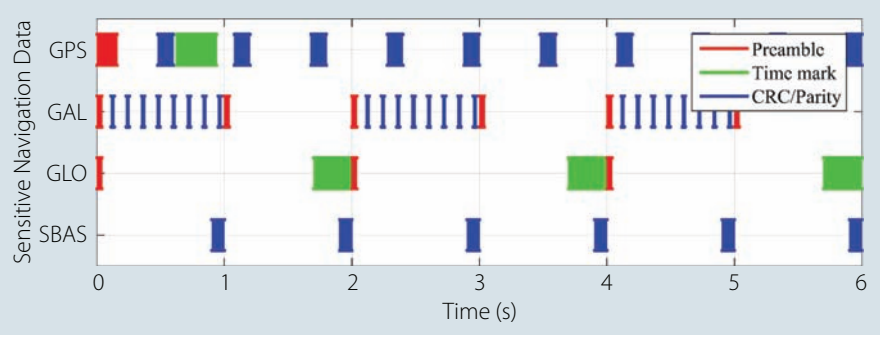


FIGURE 2 Position in time of various portions of sensitive data contained in each of the GPS, Galileo and GLONASS

for an authority to detect or locate the jamming source; it may also be possible that the interference pattern can be made sufficiently sparse that the target receiver, although experiencing a DOS, might not reliably assert that it is experiencing interference.

Here, the current Galileo E1BC and GPS L1C/A signals are studied, seeking to identify how the adversary might target these signals, and will then analyze to what extent a DOS might be conducted.

Systematic Interference and Denial of Service Attacks

The methodology chosen for the generation of harmful pulse-patterns is based on denying navigation capability of the receiver, rather than denying the signal itself. To produce a PVT solution, a receiver generally needs to extract the ephemeris from each satellite and the time-of-week (TOW) from at least one satellite. This work examined the design of interference pulse patterns which might disrupt this process.

Sensitive navigation data

A TOW message is broadcast by all GNSS signals at regular intervals, and generally occupies a very small portion of the overall navigation message. In the case of GPS L1 C/A the TOW is broadcast in an unencoded form once per subframe, whereas for Galileo E1B, it is encoded, and broadcast once per pair of pages. Thus, the denial of TOW for the GPS L1 C/A signals requires either the denial of the subframe synchronization, or denial of the raw data itself. In the case of Galileo, the TOW might be denied by either denying page synchronization, or by inducing errors in the symbol decoding process. The basic details of the navigation messages, as shown in **Figure 2**, are as follows.

GPS: The L1 C/A preamble is an 8 bit sequence (160 milliseconds) transmitted every 6 seconds. The GPS parity is composed of 6 bit (120 milliseconds) transmitted every 600 milliseconds (navigation data word). Checking the consistency of two subsequent preambles, as well as the 10 parity checks in between, is a commonly accepted mean of synchronizing to the 6 seconds boundary.

Galileo: The E1B signal transmits a plain 10 symbol synchronization sequence (40 milliseconds) every second. It is interesting to see that GPS and Galileo synchronization sequences hardly overlap in time. The Galileo message CRC is FEC encoded and then spread by an interleaver. The E1B receiver de-interleaves the data and runs a Viterbi decoder to retrieve the 120 bit/sec of I/NAV. The identification of a word results in resolving a 2 seconds time ambiguity, where certain words contain the time of week and/or week number.

Considerations for Navigation Message Authentication: Although the example examined here is that of denial of the PVT through the denial of the TOW, there are many other parts of the navigation message that could be targeted. In particular, it is worth mentioning the recent interest in the use of cryptographic methods for the protection of the navigation data. These methods typically require the inclusion of a significant number of cryptographic data bits in the navigation message, either as additional navigation data words or pages. This cryptographic data can be the order of several hundred bits, and generally has an all-or-nothing property, where any single bit error can render the entire message useless. For example, cryptographic keys can be several hundred bits in length, and digital signatures can be 300 to 600 bits in length. In both these cases, a single bit error is sufficient to corrupt them.

At present, data such as the ephemeris is broadcast piecewise, in short packets (words or pages), and repeated very frequently. Each ephemeris can be recovered piece-by-piece over time. In contrast, many proposals for GNSS message authentication have suggested that the cryptographic data be non-repeating, in order that it provide some secondary spoofing-detection, or "carry-off" protection. Following these recommendations might render the message authentication data highly sensitive to systematic-jamming, where even very sparse interference might render the authentication function unavailable. If the availability or validity of the PVT is then associated with, or conditioned upon the correct verification of the navigation message authenticity, then this PVT might be denied quite easily, and covertly. This might compare very poorly with the resilience enjoyed by current receivers, especially those that utilize extended ephemeris or assistance data.

Design of Interference Pulse Patterns

The object of this section is to identify an interference signal that will deny the extraction of the TOW from the above signals using the least amount of energy possible such that the target receiver either remain unaware of the jamming attack; might be unable to effectively mitigate the jamming signal. To simplify the problem somewhat, the jamming signal is restricted to be an on-off-keying of a chirp interference signal, transmitting pulses of fixed duration equal to some integer milliseconds.

Two particular examples are explored here: GPS L1 C/A which is subjected to pulsed interference across the broadcast TOW, and the case of Galileo E1B, which is subject to pulsed interference across a series of symbols spaced according to the symbol interleaver, and are depicted in **Figure 3**. The GPS pulse pattern has been aligned with the 17-bit TOW and consists of six 20-millisecond pulses evenly spaced across a period of 240 milliseconds. The Galileo pulse pattern consists of fifteen 4-millisecond pulses, spaced according to the Galileo 8 × 30 block interleaver, such that all 12 pulses appear consecutively once the received symbol stream has been deinterleaved.

This particular choice of pulse patterns is somewhat arbitrary, and has been selected based on some simple experiments. A more thorough design might carefully weigh the choice of number of pulses, pulse duration, and instantaneous interference power, to find a pattern which provides the highest probability of inducing bit errors, with the minimum probability of being detected. This will depend on the monitoring techniques of the receiver - including the carrier-to-noise density (C/N_0) estimator and tracking loop design.

To align these pulse patterns with the received GNSS signals, they are broadcast with a delay relative to the edge of a GPS 6 second boundary. All GNSS satellites broadcast their messages in synchronous, and all have a range between 18,000 and 24,000 kilometers, depending azimuth and elevation, this fixed delay was set to 67 milliseconds, or approximately 20,000 kilometers.

Note that the maximum variation between nearest and furthest satellite results in a misalignment of less than 20 milliseconds, and so the pulse pattern applied to the GPS L1 C/A message will still overlap completely with the 17 bit TOW message. Similarly, owing to the nature of the block interleaver used for Galileo E1B, when the pulse pattern is shifted relative to the encoded symbols, provided they still overlap with a single page, the receiver will deinterleave to a continuous stream.

Anatomy of a Systematic Jammer

Central to any jamming device is the interference generator. In the systematic jamming device envisaged here, the key to its effectiveness is the interference pulse pattern, rather than the modulation of the interference signal itself, and so it is assumed that the source is similar to a typical chirp jammer, as depicted in **Figure 4**. These devices are remarkably simple, consisting of little more than a crystal, a VCO and a power amplifier. As can be seen from the exploded view in Figure 4, the device comprises only a handful of discrete components. Elaboration to a systematic jammer would involve on-off-keying the output of such a device. This suggests that the cost and complexity of a systematic-jammer would be driven by the inclusion of a GNSS receiver, rather than the actual generation of interference.

Figure 5 shows the measured spectrum of the jammer depicted in Figure 4. The interference signal has a chirp modulation with a bandwidth of approximately 40 megahertz centered at L1. The amplitude varies slightly with frequency such that the chirp period can be clearly identified as approximately 20 microseconds. Even a very small device such as this is capable of creating a powerful wideband interference that poses a significant threat to typical GNSS receivers.

Until very recently, the only widely available transceiver option existing for radio amateurs and navigation/telecommunication engineers was the Ettus product line: the USRPs. More recently the technological advances in the integration of RF components into single multi-modal chips (mostly driven by the 3G/4G and DTV market) have enabled the design of relatively simple, highly versatile low cost SDR peripherals. A comprehensive review of such hardware is not appropriate here. Two commercially available transceivers were used in laboratory experiments. The most relevant specifications for these two devices are presented in **Table 1**.

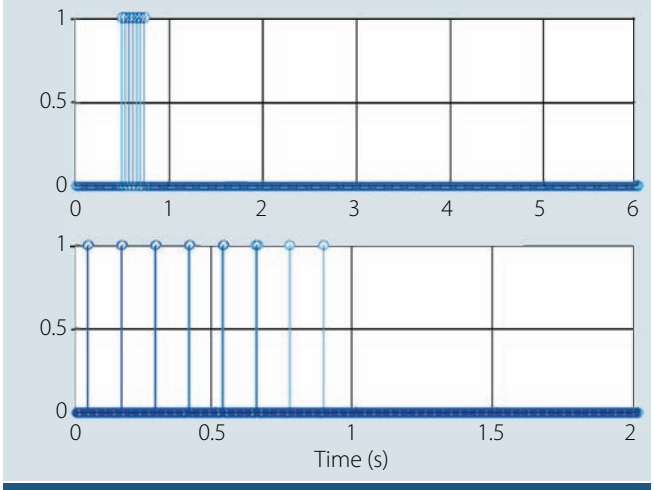


FIGURE 3 Example pulse patterns for the systematic jamming of the GPS L1 C/A (top) and Galileo E1B (bottom) navigation messages.

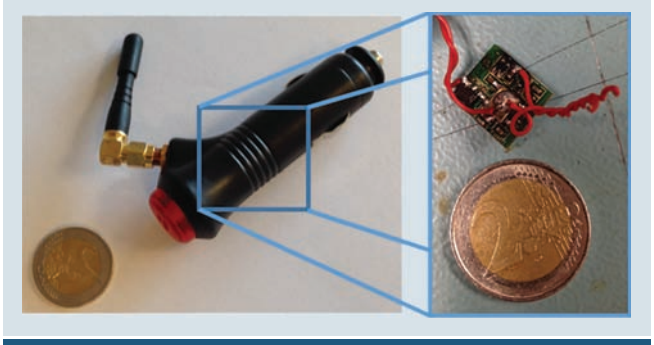


FIGURE 4 Typical in-car GNSS jammer, showing exploded-view of internal PCB. It can be seen that the device consists only of a crystal, VCO, and a few simple surface-mount components.

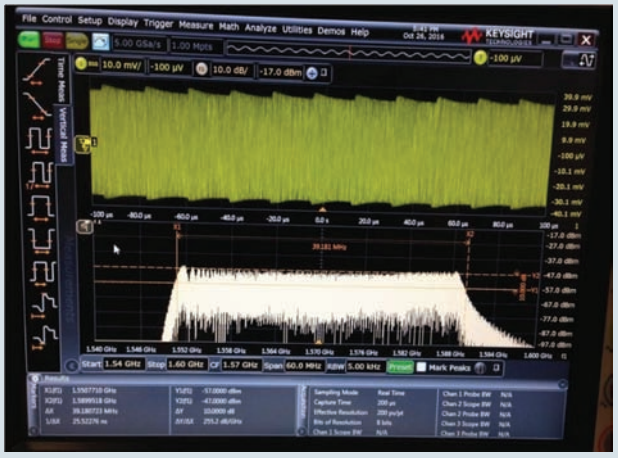


FIGURE 5 Measured spectrum of the jammer depicted in Figure 4. The interference signal has a chirp bandwidth of approximately 40 MHz centered at L1, and a chirp period of approximately 20 us.

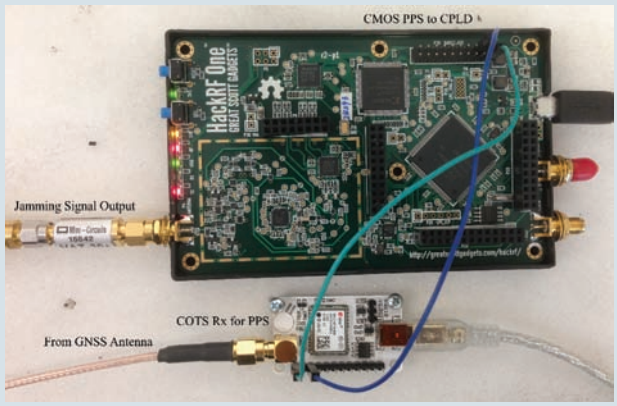


FIGURE 6 Prototype systematic jammer constructed using an open source SDR platform and a timing receiver for PPS generation.

	Transceiver One	Transceiver Two
Freq span	30 MHz - 6 GHz	300 MHz - 4.2 GHz
Bandwidth	20 MHz	28 MHz
Bits	8 I\&Q ADC/DAC	12 I\&Q ADC/DAC
Interface	USB 2.0 HS	USB 3.0
Radio	RFFC5072+MAX2837	Lime Semi LMS6602D
Baseband	CPLD + MCU	FPGA + CPU In, out, 0.5ppm
Clock	In, out, 10ppm	VCTCXO
Trigger	No (but added)	Yes

Table 1 Specification of the transceivers used in the tests

Rather than develop and integrate the hardware required for a systematic-jammer, an equivalent model was developed based on the PPS-triggered broadcast of a pre-generation of an intermediate-frequency dataset containing the required pulse-patterns. This offered a very simple means of experimenting with the concept, however a practical device would simply implement an on-off-keying of a jammer similar to that shown in Figure 4.

Synchronization of the Jammer with GNSS-Time

A trigger for transceiver two was added to the stock firmware released on June 2016. At the time of writing, however, transceiver one did not support triggering but, as it is an open hardware and software design, this feature was implemented. Testing for synchronization of two transmitters was performed by generating a simulated single GPS L1 C/A signal (for a satellite that was not visible at the time), and triggering its broadcast using a PPS edge, as shown in **Figure 6**. This simulated signal was then combined with live signals from the rooftop antenna and processed by a GNSS receiver. By examining the pseudorange difference between the simulated and live GNSS signals it was possible to assess the accuracy of the PPS-triggered broadcast. It was observed that the start of the broadcast was accurate to within a few hundred microseconds, but the range diverged rapidly due to the poor clock quality of the transmitter. This indicated that it would be necessary to periodically re-synchronize the transmission with GPS time.

Live Testing with a COTS Receiver

This section briefly describes results of a simple systematic interference test conducted on a COTS GNSS receiver. The prototype systematic jammer was constructed using a single open source SDR platform, which derived synchronization with GPS time via a timing receiver, which delivered a rising edge on a trigger once every 30 seconds, as depicted in Figure 6. Note that although this device delivered a very precise timing reference, the systematic jamming attack does not necessarily require such accuracy, indeed the GNSS propagation delay is approximated with an error of up to 10 milliseconds. Therefore, a 1 to 10 millisecond accurate reference derived from a wired or wireless network, being WiFi or a 3G mobile network, would suffice. The test consisted of a conductive combination of a live GNSS feed from a roof mounted antenna with a systematic interference signal. The receiver under test was configured to deliver raw observations to a host PC for post processing.

Denial of GPS L1 C/A PVT

In the first test, the ability of the systematic jammer to deny observations and a PVT from GPS L1 C/A was examined. The experimental setup described above was used, and the pulse pattern depicted in Figure 3 (top) was used. The prototype jammer was powered up and allowed to initialize and align with GNSS time. Next the receiver under test was issued a cold-start command and its behavior was observed. The test was repeated with progressively increasing interference

power until a power level was established at which the receiver was unable to produce a PVT, which was observed to occur at an instantaneous interference to noise floor level of approximately 30 decibels.

A trace of the 11 GPS satellites being tracked by the receiver are shown in **Figure 7**, where it can be seen that the received C/N0 for the L1 C/A signal ranges from 49 to 35 decibel-hertz, but experiences brief reductions in power of approximately 6 decibels. During the entire test, the receiver was unable to provide a sufficient set of observations and ephemerides such that a PVT could be computed. Unfortunately, it was not possible to gain enough visibility into the internal receiver functionality to determine exactly which information was successfully extracted. It would have been helpful to understand whether ephemeris, almanac, health status and other variables were available, or whether the annihilation of the TOW and subsequent CRC failure rendered all data unavailable. Nonetheless, the results confirm that it is possible to deny a GPS L1 C/A based PVT via the targeted jamming of just a small portion of the navigation message. Beyond the results presented here, a similar systematic interference test was conducted and configured to run continuously over a 24-hour period, such that the receiver experienced a complete change in the visible constellation. Again, it was found that the receiver was unable at any point to provide a PVT despite the fact that the receiver was capable of acquiring and tracking all signals visible with only a minor degradation to the C/N_0.

Denial of Galileo E1B PVT

The second test conducted was designed to assess the ability of the systematic jammer to deny observations and a PVT from the Galileo E1B signals. The pulse pattern was further changed to that of Figure 3 (bottom) and an experimental setup similar to the GPS case was used. However, due to the low availability of healthy Galileo satellites, the live GNSS feed from the roof antenna was replaced with a simulated signal sourced from a multi-constellation simulator. In this case the pulse pattern significantly more distributed in time, being spread relatively evenly across the I/NAV odd page. This particular pulse pattern was shaped according to the interleaving pattern, rather than being aligned with a particular data word, with the intention that once it is deinterleaved, it will appear as a continuous stream of symbol errors arriving at the decoder.

Interestingly, the ability of this approach to deny the navigation message is relatively insensitive to its alignment with the beginning of the page. Provided the complete set of pulses are received within one page, they will be de-interleaved into a continuous stream.

A screenshot from one of the tests is shown in **Figure 8** which includes a trace from eight Galileo and nine GPS satellites. As expected, the Galileo E1B message has been denied by the systematic interference, as indicated by the blue color-coding of the figure. Two interesting observations were made during this test. First, it was noted that the reception of the GPS L1 C/A signal was relatively unaffected. Eight of the nine GPS satellites report useful observations, and the receiver steadily provided a GPS-based PVT. The second particularly striking observation is that the C/N_0 reported by the receiver under test does not exhibit any significant variation either for GPS or for the Galileo satellites. A C/N_0 in the range of 48 to 49 decibel-hertz was reported for all Galileo satellites, yet the

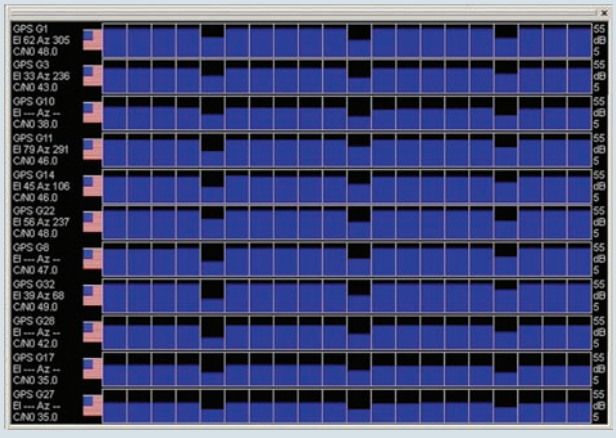


FIGURE 7 Screenshot from the GNSS evaluation software during a systematic interference attack on GPS L1 C/A. Signals that are tracked are presented in blue, and those for which the navigation message has been recovered are presented in green.

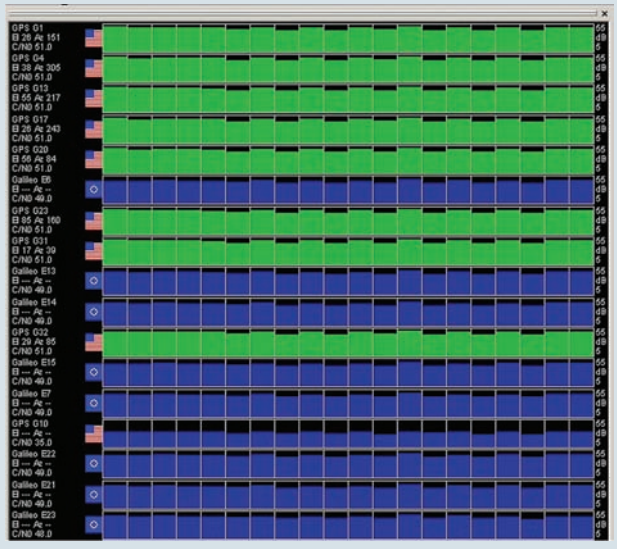


FIGURE 8 Screenshot from the GNSS evaluation software during a systematic interference attack on Galileo E1B. Signals that are tracked are presented in blue, and those for which the navigation message has been recovered are presented in green.

Signal	TPulse	NPulse	TPatt	KSyst
GPS L1 C/A	20 ms	6	6s	17 dB
Galileo E1B	4 ms	15	2s	15 dB

Table 2 Effective reduction in required average interference power when employing systematic jamming

receiver was unable to extract navigation data from any of them. One reason for this is that the interference is relatively sparse in time and its effect is smoothed by the C/N_0 estimation process.

A few interesting conclusions are drawn from these results. We note that is possible to deny the use of one kind of GNSS signal, in this case, Galileo E1B, while leaving the other, in this case GPS L1 C/A, relatively unaffected, even when they occupy the same RF band. This appears to be due to the relative orthogonality of the navigation message structures, owing to their significantly different symbol periods, 4 milliseconds and 20 milliseconds, and the fact that one employs FEC while the other does not. It is also clear that the observation of C/N_0 may not be a useful means of interference detection, given that the C/N_0 level observed on the GPS and Galileo signals was virtually identical, yet the impact of the interference on the receiver's ability to process the signal is drastically different.

Power, Energy and Synchronization

The probability of a bit or symbol error occurring is a very nonlinear function of the instantaneous interference power, however this probability of error saturates at 0.5. To achieve a more reliable denial of the navigation message, more symbols must be targeted, where the probability that the message is corrupted is given by:

$$P_{Err} = 1 - 0.5^{N_{Pulse}} \quad (1)$$

where N_{Pulse} denotes the number of corrupted symbols. This probability tends to unity quite rapidly. Naturally, the total interference energy required increases as a linear function of the number of symbols:

$$E_{Int} = P_{Ind} N_{Pulse} T_{Pulse} \quad (2)$$

where T_{Pulse} the pulse periods, being equal to the symbol or bit period. An astute adversary will tune this energy effecting a trade-off between the probability that the navigation message is denied, and the probability that the interference power will alert the receiver to the attack. In effect, by using a systematic interference, an adversary can reduce the total interference energy, or average interference power required to render the PVT unavailable. The reduction can be computed relative to a continuous interference signal, by expressing the average duty-cycle of the interference:

$$K_{Syst} = -10 \log_{10}\left(\frac{N_{Pulse} T_{Pulse}}{T_{Patt}}\right) \quad (3)$$

where T_{Patt} is the repetition period of the interference pattern, being 6 seconds for GPS L1 C/A and 2 seconds for Galileo E1 B. The interference configuration for both the GPS L1 C/A and Galileo E1B are summarized in **Table 2**, where it is suggested that the effective gain of applying systematic jamming, as opposed to continuously broadcast jamming, is in the region of 15 to 17 decibels. Moreover, although the results here have been generated using a tightly synchronized transmitter, the principle of operation of the systematic jammer would permit synchronization errors in the region of 1 to 10 milliseconds. Notably, at this level of timing error, the jammer may no longer need to avail of position information.

Conclusion

The literature to date has primarily considered the two extremes of GNSS vulnerability, being either a very simple jamming attack, or a very complicated spoofing attack. Simple jamming, as we know it today, is a very easy attack to launch, but it is also very easily detected, readily localized, and often relatively easily mitigated. Spoofing, although very possible, and not necessarily difficult, is considerably more difficult than jamming. In the short term, if denial of service through simple jamming becomes non-viable, it is not unreasonable to expect this threat to evolve. There appears to be a middle-ground between jamming and spoofing, that might thwart current detection, localization and mitigation techniques. It appears to be very accessible to a malicious attacker, as it only requires commercial, off-the-shelf components, and some basic integration; yet it can pose a significant threat to a naïve receiver implementation. This increased threat comes at a very small increased attack cost and complexity, and has the potential to disrupt many location-based services, by imposing an undetectable partial (data recovery) or full (position and timing) denial-of-service. Preliminary results suggest that this attack methodology is feasible and, under certain conditions, may be quite effective when targeting a naïve receiver.

It is interesting to note that through interference signal design, it is possible to deny signals from one constellation why not negatively impacting signals from another, even when these signals share the same spectrum. Because this is achieved by carefully choosing the on-off-keying pattern, it is likely that this technique can be extended to target specific satellites from a given constellation.

This work represents only a very preliminary examination of the concept, but does seem to highlight the fact that it may be naïve to assume that the jamming threat will not evolve in reaction to anti-jamming technology. The notion that jamming devices might be designed in direct response to anti-jamming techniques might open a new avenue of research into the more game-theoretic aspects of resilient GNSS receivers. It might further invigorate the use of technologies such as antenna diversity, or synthetic aperture antennas, or adaptive interference mitigation techniques.

Manufacturers

When the authors note that a jammer may be equipped with a simple commercial GNSS receiver that provides accurate position, time and satellite ephemerides, they are referring to the

u-blox "M8 concurrent GNSS timing modules," <www.u-blox.com/en/product/neolea-m8t-series>.

Additionally, in the section on Live Testing with a COTS Receiver, the timing receiver is one manufactured by **u-blox**, Thalwil, Switzerland, and Figures 8 and 9 refer to the u-blox u-center GNSS evaluation software.

The open source SDR platform used in the Live Testing with a COTS Receiver and mentioned in Figure 6 is a HackRF One from **Great Scott Gadgets**, Evergreen, Colorado. HackRF One is also referenced as Transceiver One in Table 1.

Transceiver Two in Table 1 refers to bladeRF, **Nuand LLC**, Rochester, New York.

The simulator used in the Denial of Galileo E1B PVT Section is a Spectracom GSG-6 Series Multi-Constellation simulator from **Spectracom**, Rochester, New York.

Additional Resources

[1] Amin, M. G., and P. Closas, A. Broumandan, and J. L. Volakis. "Vulnerabilities, threats, and authentication in satellite-based navigation systems [scanning the issue]." *Proceedings of the IEEE,* 104(6):1169-1173, 2016.

[2] Curran, J., M. Navarro, M. Anghileri, P. Closas, and S. Pfletschinger. "Coding aspects of secure GNSS receivers." *Proceedings of the IEEE,* 104(6):1271-1287, 2016.

[3] Dovis, F., "GNSS Interference Threats and Countermeasures." Artech House, Boston, 2015.

[4] Fontanella, D., R. Bauernfeind, and B. Eissfeller. "In-car GNSS jammer localization with a vehicular ad-hoc network." In *Proceedings of the 25th International Technical Meeting of The Satellite Division of the Institute of Navigation,* pages 2885-2893, September 2012.

[5] Humphreys, T. E., J. Bhatti, D. Shepard, and K. Wesson. "The Texas spoofing test battery: Toward a standard for evaluating GPS signal authentication techniques." In *Proceedings of the 25th International Technical Meeting of The Satellite Division of the Institute of Navigation,* pages 3569-3583, September 2012.

[6] Humphreys, T. E., B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner. "Assessing the spoofing threat: Development of a portable GPS civilian spoofer." In *Proceedings of the 21st International Technical Meeting of the Satellite Division of The Institute of Navigation,* pages 2314-2325, September 2008.

[7] Johnson, M., and R. Erlandson. "GNSS receiver interference: Susceptibility and civil aviation impact." In *Proceedings of the 8th International Technical Meeting of the Satellite Division of The Institute of Navigation,* pages 781-791, September 1995.

[8] Kraus, T., R. Bauernfeind, and B. Eissfeller. "Survey of in-car jammers - analysis and modeling of the RF signals and IF samples (suitable for active signal cancellation)." In *Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation,* pages 430-435, September 2011.

[9] Mitch, R. H., R. C. Dougherty, M. L. Psiaki, S. P. Powell, B. W. O'Hanlon, B. W. Bhatti, and T. E. Humphreys. "Signal characteristics of civil GPS jammers." In *Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation,* pages 1907-1919, September 2011.

[10] Motella, B., S. Savasta, D. Margaria, and F. Dovis. "An interference impact assessment model for GNSS signals." In *Proceedings of the 21st International Technical Meeting of the Satellite Division of The Institute of Navigation,* pages 900-908, September 2008.

[11] NSL, Spirent, "Detector", www.spirent.com/Products/GSS200D-Detector, Accessed 2016.

[12] Psiaki, M. L., and T. E. Humphreys. "GNSS Spoofing and Detection." *Proceedings of the IEEE,* 104(6):1258-1270, 2016.

[13] Pozzobon, O., C. Sarto, A. Dalla Chiara, S. Pozzobon, G. Gamba, M. Crisci, and R. T. Ioannides. "Developing a GNSS position and timing authentication testbed GNSS vulnerability and mitigation techniques." In *Inside GNSS* article, January 2013.

[14] Samson, J., L. Musumeci, and F. Dovis. "Performance assessment of pulse blanking mitigation in presence of multiple distance measuring equipment/tactical air navigation interference on global navigation satellite systems signals." *IET Radar, Sonar and Navigation,* 8(6):647-657, July 2014.

[15] Spirent, "Simsafe", www.spirent.com/Products/simsafe, Accessed 2016.

[16] Wildemeersch M., and J. Fortuny-Guasch. "A laboratory testbed for GNSS interference impact assessment." In *Proceedings of the 22nd International Technical Meeting of The Satellite Division of the Institute of Navigation,* pages 49-54, September 2009.

[17] Curran, James T., Bavaro, Michele, Closas, Pau, Navarro, Monica, "On the Threat of Systematic Jamming of GNSS," *Proceedings of the 29th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2016),* Portland, Oregon, September 2016, pp. 313-321.

Authors

James T. Curran (jamestcurran@ieee.org) received a B.E. in electrical & electronic Engineering and a Ph.D. in telecommunications from the Department of Electrical Engineering, University College Cork, Ireland. He worked as a senior research engineer with the PLAN Group in the University of Calgary, Canada, and as a grant-holder at the Joint Research Centre (JRC) of the European Commission (EC), Italy. James is currently a radionavigation engineer at the European Space Agency in the Netherlands. His main research interests are signal processing, information theory, cryptography, and software defined radio.

Michele Bavaro received his master degree in computer science from the University of Pisa, Italy. Shortly afterwards he started his work on Software Defined Radio technologies applied to navigation, first in Italy, then in The Netherlands at the European Space Agency. In the United Kingdom he worked for NSL on several projects being directly involved with the design, manufacture, integration, and test of radionavigation satellite system (RDSS) equipment and supporting customers in the development of their applications. After working on his own consulting firm, mostly on SDR and low cost precision positioning, he was appointed as technical officer at the Joint Research Center (JRC) of the European Commission. Michele works now at Swift Navigation in California for the measurement engine team.

Pau Closas (pau.closas@northeastern.edu) is an assistant professor at the Department of Electrical and Computer Engineering, Northeastern University, Boston, MA. He received his MS and PhD in electrical engineering from the Universitat Politècnica de Catalunya (UPC) in 2003 and 2009, respectively. He also holds a MS degree in advanced mathematics and mathematical engineering from UPC since 2014. His primary areas of interest include statistical signal processing and robust stochastic filtering, with applications to positioning systems and wireless communications. He is the recipient of several awards, including the 2014 EURASIP Best PhD Thesis Award and the 2016 ION Early Achievement Award.

Dr. Monica Navarro is a Senior Researcher at the Centre Tecnologic de Telecomunicacions de Catalunya within the Communication Systems Division. She received the MSc degree in Telecommunications Engineering from Universitat Politecnica de Catalunya in 1997 and the PhD degree in Telecommunications from the Institute for Telecommunications Research (ITR), University of South Australia, in 2002. From Oct. 1997 to Dec. 1998 she was a Research Assistant at the Department of Signal Theory and Communications at the UPC, where she worked on the development of fractal shape multiband antennas for wireless cellular communications systems. She has also been part-time lecturer at the Universitat Pompeu Fabra, Barcelona. Her primary areas of interest are on digital communications and signal processing, particularly on iterative information processing, adaptive transmissions and coding techniques, signal processing for synchronization, estimation and detection theory with applications to radio communications systems, including wireless mobile communications, deep-space communications, wireless sensor networks, and positioning applications. IG