

In 2008, the UK government eLoran tests used a two-watt GPS jammer to block satellite signals over the 30-kilometer-long section of the North Sea (shown in orange). Jammers of the same power are available on the Internet.

Why we should stop taking GNSS for granted, start worrying about signal failure and malicious jamming, and *do something about it!*

DAVID LAST

Quietly but surely, positioning, navigation and timing are being taken for granted.

The location information that GPS gives us is now at the heart of our transportation capabilities, distribution industries, just-in-time manufacturing, emergency service operations, not to mention mining, road-building, and farming.

Even more sobering — and what few members of the public know — GPS provides the high-precision timing that helps keep our telephone networks, the Internet, banking transactions and even our power grid on line.

But my job in this article is not to praise GPS. Rather, I am to be the bringer of bad news. To identify weaknesses of our technology, to cry, “Woe, Woe and thrice Woe!”

My message is simple, if perhaps surprising: Should we lose the utility that is GPS, we may well lose critical electrical power supplies and communications, and then we could face a dark, silent, and dangerous world.

But is there any danger in real life? We experience daily how wonderfully reliable GPS is. The public just loves it, and people do now believe in its technical perfection.

Consider the mythology that has grown up around this amazing technology, fuelled by mass media such as movies and television. They are perhaps making too much of a good thing, such as described in the sidebar, “Four Popular Myths of GNSS.”

Even many professionals, with considerable experience of the precise and reliable performance of GPS, begin to act as if it were indeed infallible.

Such attitudes belie an excess of confidence. GPS — and, by extension, any GNSS — *is* vulnerable.

The Achilles heel of all GNSS systems is the extremely weak signals that reach the receiver. Each satellite transmits no more power than a car headlight, and yet must illuminate nearly half the earth’s surface from 20,000 kilometers out in space.

This can lead to problems.

Large ships have integrated bridges and electronic chart displays driven directly by GPS.

One man has fingertip control of a 100,000-ton vessel, at 25 knots. He will sail it in fog with confidence through the busiest sea-lanes in the world.

But what happens when one-tenth of one-thousandth of a watt of radio frequency gets into the wrong place, interfering with the GPS signals? Quietly, the chart display in this floating metropolis begins to tell lies and presently other systems fail, leaving that one man to revert unexpectedly and belatedly to the difficult and no longer familiar practice of radar navigation.

GPS failures are not something we commonly experience. But they do happen. They already *have* happened.

Clock Failure

On New Year's Day 2004, when not many people were sober or out and about, the last atomic clock on GPS satellite SVN23 gave up the ghost. (Perhaps it had had a rough night, too!)

Because of the kind of failure and the location of the satellite, it took nearly three hours for the GPS system to tell receivers to exclude its signals.

The result for GPS receivers in Europe was position errors that started slowly and without warning, but built up insidiously to between 10 and 40 kilometers (6–25 miles).

The maritime automatic identification system showed ships actually travelling over land!

Now, mariners do have a protection service for such situations. Coastal radio stations can automatically alert their GPS receivers when a satellite fails. On this occasion the system worked fine and kept the GPS service really accurate.

EGNOS, the European satellite-based WAAS-like GPS augmentation system, and the receiver autonomous integrity monitoring (RAIM) function in aviation receivers also performed well.

But that day clearly showed the hazard of operating GPS without an integrity monitoring system.

What about Galileo? Would the European GNSS have solved the 2004 clock failure? It certainly would have helped receivers designed to compare the systems to detect the GPS system breakdown. But receivers using that faulty GPS satellite would still have given very large errors.

But the failures that satellites like SVN23 have experienced aren't the main problem. It's the vulnerability of those weak GNSS signals to interference — whether natural, unintentional, or malicious — that puts the system at risk.

For example, on December 6, 2006, the most powerful solar flare ever recorded simply came out of the blue. The Sun radiated radio noise of such intensity that deafened GPS receivers stopped working across the entire sunlit side of the earth.

WAAS, the U.S. Wide Area Augmentation System that provides signal corrections for aviation, was out of service for 15 minutes.

Four Popular Myths of GNSS

Let's take a look at that great work of contemporary English literature, Dan Brown's 2003 mystery, *The Da Vinci Code*.

We thrill as the evil Captain Fache uses a tiny GPS to track our unknowing Hero and his Lady Friend as they explore an underground crypt far beneath the Louvre in Paris.

That GPS is accurate to two feet. Now, this scene manages to combine in a single paragraph four great myths concerning GPS:

1. GPS is itself a tracking system that can tell those busybodies in Whitehall just where we all are
2. It works always and everywhere, even in mysterious underground tombs.
3. It has pinpoint accuracy
4. It needs just a single satellite.

That's a pretty good collection of errors for a book that purports to be a revelation of truth, hidden from us for centuries.

No wonder people have infinite trust in GPS!

Solar flares like that affect all our satellite navigation systems, including Galileo.

But even if the satellites and the ionosphere are working perfectly, when you are listening for something as faint as a GNSS signal, even a whisper in your ear will drown it out.

Of course, the world is full of very loud interference, as well as whispers.

A Tempting Target

In 2001, the United States Transportation Department released the Volpe Report, "Vulnerability Assessment of the Transportation Infrastructure Relying on GPS."

The report said that radio interference, intentional or unintentional, could be reduced but never eliminated. That losing GPS would cause severe safety and economic damage to the United States. And that, for those reasons, GPS is a tempting target to individuals, groups, or countries hostile to the United States.

Unintentional interference is relatively common in some places. Northern Italy used to be notorious for interference to GPS from high-power TV stations — mostly unlicensed and run by the Mafia, I'm told.

But it's the uncommon or unexpected interference that may produce the most adverse effects. For instance, on January 22, 2007, GPS suddenly disappeared for two hours across large parts of the San Diego, California area. More than 100 mobile phone transmission towers were affected and a hospital paging system went out. The first responders dealing with the incident couldn't even communicate.

It was all an accident, caused by a U.S. Navy jamming training exercise that went awry.

Meanwhile, the navigation community has long talked about the possibility of intentional interference: GPS jamming.

Over many years, we have seen strange devices appear on websites for hackers. We learned of terrorists arrested

in the U.S. with jamming equipment. We monitored the development of military jamming, saw it deployed in Iraq and watched counter-measures appear.

But for a long time, almost the only intentional jamming to affect civil GPS was deployed by governments themselves to assess the threats and develop defenses.

Now all that has changed. Consider this simple test:

Just Google “GPS” plus “Jammer” and see how many Internet “hits” you receive. It used to produce just a few results. As of February 2010, that same Google search is up to 185,000! Most hits are people selling commercial GPS jammers in what is now a thriving market.

Now, I have some first-hand experience of this development in my practice as a forensic expert witness. Recently I have handled a number of jamming devices seized by the police from criminals.

Almost every high-value load on a truck or a trailer is protected by a GPS tracking system. So, too are rental cars and luxury vehicles that might be stolen and exported for sale in Eastern Europe.

Criminals use jammers to disable and defeat those tracking systems and so steal the vehicles and their contents. (See **Figure 1**.) This device is a low-power transmitter that blocks GPS reception. It costs less than €100 (US\$135), while the goods stolen in recent cases have cost millions.

This jammer radiates less than a milliwatt of power in the spectrum centered on the GPS L1 frequency, and has a range of just tens of meters. But here’s an interesting thing: that transmission blocks not only civil GPS, but also the wider military P/Y signal. Then, for good measure, it takes out all the Galileo L1 band and most of the GLONASS frequencies.

To complete the job, the Bad Guys can also obtain this inexpensive jammer (shown in photo at right) to remove a target vehicle completely from the radar by jamming mobile phones that could be used to call for assistance and be tracked using cell-site analysis.

The little device blocks DCS, 3G, and GSM mobile phones, as well as GPS. Really, excellent value for the money!

On the Street

But if you want bang for your buck, why not try one of the two-watt jammers now available on the street. That’s the same jamming power used in recent UK government tests to block GPS over the 30-kilometer-long section of the North

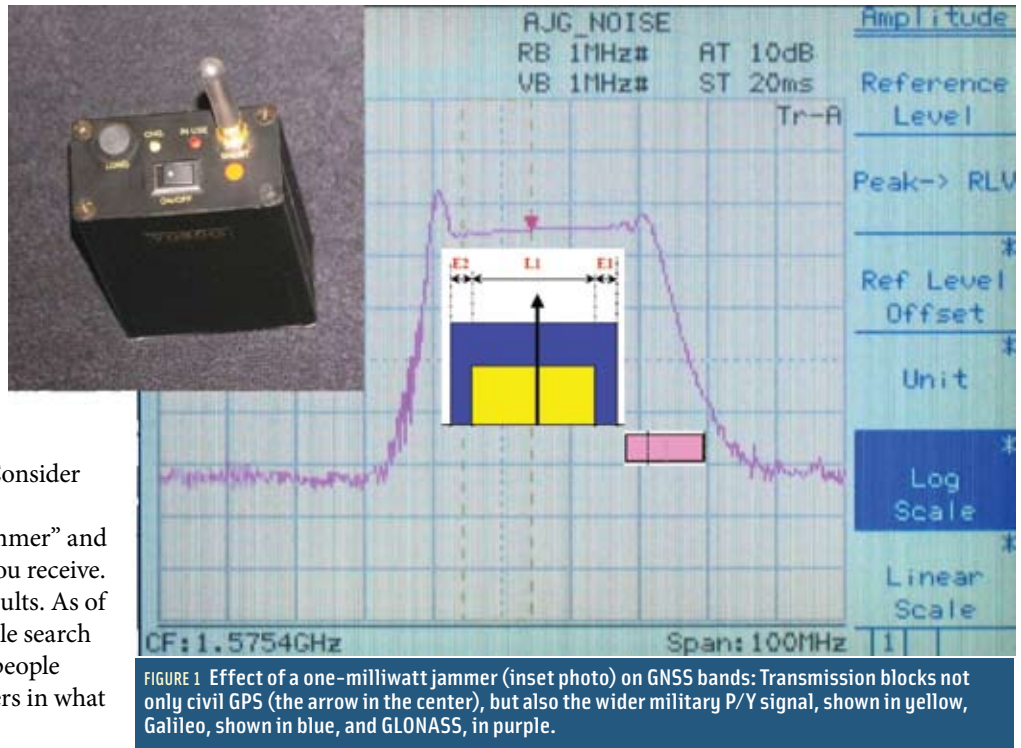


FIGURE 1 Effect of a one-milliwatt jammer (inset photo) on GNSS bands: Transmission blocks not only civil GPS (the arrow in the center), but also the wider military P/Y signal, shown in yellow, Galileo, shown in blue, and GLONASS, in purple.

Multi-purpose jammer blocks GPS signals as well as DCS, 3G and GSM mobilephones



Sea shown in orange in the graphic on the opening page of this article.

Will more GNSS signals help? Several systems in addition to GPS are under way. Galileo will use multiple frequency bands. So, jamming the GPS L1 signal alone won’t work. And with the new signals and frequencies on GLONASS and China’s Compass system, plus augmentations, within five years



FIGURE 2 Example of jammers available on the Internet

or so we may have more than 140 GNSS satellites in orbit (including regional and augmentation systems).

By 2015, the sky will become dark with satellites, the sunlight will dim, and Global Warming will be forestalled!

Well, whatever the collateral benefits, those satellites are still to come, but the jammers for them are already here.

The device shown in **Figure 2** takes out the L1, L2 and L5 GNSS bands. It's on the street (well, a virtual street of the World Wide Web), and you don't even have to pay sales tax!

All of these jammers are relatively simple devices yet highly effective with civil receivers. They are readily available, and

they're being sold and used. They can attack the myriad applications of GPS, including critical timing systems. They render civil GPS-based security systems highly vulnerable to attack.

More seriously still, the über-techies are now successfully transmitting fake GPS signals: spoofing civil GPS. A receiver locks onto the spurious signals, and the spoofer effectively controls the user's device.

Security technologist and author Bruce Schneier discusses how far this has come in his blog, "Schneier on Security." He said that, in an experiment, a desktop computer attached to a GPS satellite simulator was used to create a false signal, and, in a later experiment, [the operator] spoofed GPS signals at ranges over three-quarters of a mile at Los Alamos, New Mexico.

So, we will have to watch out for criminals who use spoofing to make it appear that a hijacked vehicle is following its original route . . . or scofflaws using spoofers to avoid GNSS-based road-user pricing systems.

Defenses Against the Dark Arts

So, how can we defend ourselves — short of calling in James Bond or Harry Potter? Many look to the law to detect and prosecute the jammers. But it's not easy to detect a few milliwatts of white noise against a background of natural white



To the Rescue: eLoran?

What happens when GPS or GNSS has a bad-hair day due to jamming or interference?

Radiating very high-powered signals at low frequency, the land-based transmissions of an enhanced Loran (eLoran) system offer an excellent complement to GPS with their low-powered, microwave frequency signals, eliminating common modes of failure.

eLoran technology can be built into a satellite navigation receiver and seamlessly take over when necessary, driving the same user display. The system can also replace the high-precision timing in critical telecom networks and power grids currently supplied by GPS.

Just as GPS developed from earlier satellite systems, eLoran grew out of Loran-C. It uses the same stations, modernized for the digital era with high-reliability equipment, and a data system that can achieve accuracy of 10 meters in differential operation.

The signals of Loran-C, once the world's most-used long-range navigation system,

are broadcast in the Far East, Middle East, and northern Europe. Together with the North American stations, they supported 72 percent of the world's 50 busiest ports until the U.S. service was turned off earlier this year.

A team representing 40 international government agencies, companies, and universities and led by the U.S. Federal Aviation Administration developed eLoran technology in response to the 2001 Volpe Report on GPS vulnerability.

The team showed that existing Loran-C assets modernized to radiate eLoran, plus high-performance digital receivers, could meet a wide range of U.S. national and international requirements. These included harbor entrance maneuvering by ships, non-precision instrument approaches by aircraft, and the Stratum 1 frequency standard and UTC timing required by the telecommunications industry.

The FAA said eLoran could "mitigate the operational effects of a disruption in GPS services, thereby allowing the GPS users to retain the benefits they derive from their use of GPS."

Most of the old Loran-C stations in the U.S. were modernized, making them suitable for conversion to eLoran. A high-level independent assessment team led by Charles Stark Draper Prize winner (and the original GPS Joint Program Office commander) Brad Parkinson concluded unanimously that this was the way ahead. Parkinson himself said, "I am a supporter of having a backup radionavigation system,

and the only backup system I can see is Loran".

In 2008, the Department of Homeland Security announced that the U.S. was adopting eLoran as its national GPS backup.

A few years ago, the U.S. Coast Guard achieved a world first by demonstrating an eLoran high-integrity navigation and timing system, accurate to 10 meters (33 feet). It was compatible with GPS but immune to the loss of satellite signals. Despite this rapid progress, the United States closed down most of its Loran-C stations earlier this year, leaving eLoran with an uncertain future in that nation.

And the rest of the world? The 2008 U.S. announcement to proceed with eLoran led to an upsurge of interest in converting stations and operations from Loran-C to eLoran. The United Kingdom, stating that "robust, reliable and high-performance positioning, navigation and timing (PNT) is the lifeblood of modern society's critical infrastructure", deployed a new station for eLoran.

Together with Loran-C stations in France, Germany, Norway and the Faroe Islands, the UK now provides a prototype eLoran service around the clock.

As concerns about GNSS vulnerability to interference and jamming grow, so do calls for eLoran to be adopted as a component of the future radionavigation mix, integrated with GPS plus either Galileo, modernized GLONASS or Compass-Beidou.

noise. And spoofers make it even more difficult: how do you locate a signal that looks just like a GPS signal?

Others believe a much less vulnerable fall-back is needed: a solid alternative source of position, navigation, and timing.

If that can take over when GPS is not available, it takes the reward out of jamming, and it spoils the fun.

Road vehicle tracking systems, such as Datatrak and stolen vehicle recovery systems like Tracker with its Lojack technology, already exist. For navigation, if you already have a GNSS fix, you can hang onto it for a while with the kind of dead-reckoning and map-matching technologies used in built-in car navigators.

And many, including me, strongly support the UK's move to enhanced Loran or, more succinctly, eLoran. It offers a complete positioning system that can take over seamlessly from GNSS when it has a bad hair day and provide telecommunications timing precision as well. (See the sidebar, "To the Rescue: eLoran?")

Navigation is no longer about how to measure where you are accurately. That's easy. Now it's how to keep this critical infrastructure working reliably, safely and *robustly*.

We've seen that GNSS is vulnerable. That given the dependence on GNSS of our transportation, industry, commerce, and telecommunications, this vulnerability is a threat to our critical infrastructure.

Because all of our present and proposed sources of GNSS share technologies and radio frequencies, they also share common vulnerabilities. So, Galileo and Compass and the new GLONASS can only provide limited support to GPS or one another.


We've also seen that there are solutions, involving combinations of GNSS and other technologies.

But make no mistake: spoofing may still be a future hazard, but solar flares, unintentional interference, and most of all intentional jamming, are now real and present dangers.

This article was adapted from a keynote speech delivered by the author on February 23, 2010, at the Digital Systems Knowledge Transfer Network conference, "GPS Jamming and Interference – a Clear and Present Danger," at the National Physical Laboratory in Teddington, London, England.

Author



David Last is a radionavigation expert and consultant, past president of the Royal Institute of Navigation, and professor emeritus at the University of Bangor, Wales. Before his retirement in 2005, he headed the university's Radionavigation Group. He is a past president of the International Loran Association, a fellow of the Institute of Engineering and Technology (IET), and a Chartered Engineer (CEng). Last has published widely on navigation systems, including GPS, Loran-C, eLoran, Galileo and other GNSSes, maritime differential GPS, Argos, Decca Navigator and Omega. He holds a B.Sc.(Eng) from University of Bristol, a Ph.D from University of Sheffield, and a D.Sc. from University of Wales. He lives and works in Conwy, UK. His website is <<http://www.professordavidlast.co.uk>>. 

SLAM DANCE continued from page 58

based in part on a paper presented at the ION GNSS 2009 conference in Savannah, Georgia, USA.

Manufacturers

An EVK-5 GPS receiver from **u-blox AG**, Thalwil, Switzerland; an OS5000 digital compass from **OceanServer Technology, Inc.**, Fall River, Massachusetts, USA; an MS55490 baro-altimeter from **MEAS Switzerland SA** (formerly **Intersema Sensoric SA**), Bevaix, Switzerland; i-CARD2 RFID reader and tags from **Identec Solutions AG**, Lustenau, Austria; an MTx-28A53G25 IMU from **Xsens Technologies B.V.**, Enschede, The Netherlands.

Additional Resources

- [1] Angermann, M., and A. Friese, M. Khider, B. Krach, K. Krack, and P. Robertson, "A Reference Measurement Data Set for Multisensor Pedestrian Navigation with Accurate Ground Truth," in *Proceedings of European Navigation Conference ENC-GNSS 2009*, Naples, Italy, 2009
- [2] Arulampalam, S., and S. Maskell, N. Gordon, and T. Clapp, "A tutorial on particle filters for online nonlinear/Non-Gaussian Bayesian Tracking," *IEEE Transactions on Signal Processing*, vol. 50, no. 2, pp. 174–188, February 2002
- [3] Beaugregard, S., Widyawan, and M. Klepal, "Indoor PDR Performance Enhancement Using Minimal Map Information and Particle Filters," in *Proceedings of the IEEE/ION PLANS 2008*, Monterey, California USA, May 2008
- [4] "FootSLAM videos and reference data sets download," <<http://www.kn-s.dlr.de/indoornav>>
- [5] Foxlin, E., "Pedestrian Tracking with Shoe-Mounted Inertial Sensors," *IEEE Computer Graphics and Applications*, vol. 25, no. 6, pp. 38–46, November 2005
- [6] Foxlin, E., and S. Wan, "Improved Pedestrian Navigation Based on Drift-Reduced MEMS IMU Chip," 2010 ION International Technical Meeting, San Diego, California USA, January 2010.
- [7] Khider, M., and S. Kaiser, P. Robertson, and M. Angermann, "A Novel Movement Model for Pedestrians Suitable for Personal Navigation," in *ION National Technical Meeting 2008*, San Diego, California, USA, 2008
- [8] Krach B., and P. Robertson, "Cascaded Estimation Architecture for Integration of Foot-Mounted Inertial Sensors," in *Proceedings of the IEEE/ION PLANS 2008*, Monterey, California USA, May 2008
- [9] Krumm, J., "A markov model for driver turn prediction," in *SAE 2008 World Congress*, Detroit, MI USA. Springer-Verlag New York, Inc., 2008
- [10] Montemerlo, M., and S. Thrun, D. Koller, and B. Wegbreit, "FastSLAM: A factored solution to the simultaneous localization and mapping problem," in *Proc. AAAI National Conference on Artificial Intelligence*, Edmonton, Canada, 2002
- [11] Robertson, P., and M. Angermann, and B. Krach, "Simultaneous Localization and Mapping for Pedestrians Using Only Foot-Mounted Inertial Sensors," in *Proceedings of UbiComp 2009*, Orlando, Florida, USA
- [12] Smith, R., and M. Self, and P. Cheeseman, "Estimating Uncertain Spatial Relationships in Robotics," in *Autonomous Robot Vehicles*, I. J. Cox and G. T. Wilfong, Eds., Springer Verlag, New York, 1990, pp. 167–193
- [13] Woodman, O., and R. Harle, "Pedestrian Localisation for Indoor Environments," in *Proceedings of the UbiComp 2008*, Seoul, South Korea, September 2008. 