

The
Economist

GPS jamming

No jam tomorrow

Navigation: As the uses of satellite-positioning technology continue to grow, what can be done to stop deliberate and dangerous jamming of the signals?

Mar 10th 2011 | from the print edition



NO AEROPLANES fell out of the sky and no one died. But in late 2009 engineers noticed that satellite-positioning receivers for a new navigation aid at Newark airport in New Jersey were suffering brief daily breaks in reception. Something was interfering with the signals from orbiting global positioning system (GPS) satellites. It took two months for investigators from the Federal Aviation Authority to track down the problem: a driver who passed by on the nearby New Jersey Turnpike each day had a cheap GPS jammer in his truck.

Such devices are illegal to sell or use, but they have become popular with commercial drivers who object to their employers tracking their every move. A jammer prevents a tracking device in the vehicle from determining (and then reporting) its location and speed—but it also disrupts GPS signals for others nearby.

Although the incident did not have disastrous repercussions or make front-page headlines, it did ring alarm bells with senior aviation and law-enforcement officials. America's military developed GPS from the 1970s, and satellite-based positioning, navigation and timing (PNT) have since become crucial to all kinds of civilian infrastructure systems. Most people know that satellite signals are used by automotive "satnav" devices, but few realise how everything from aviation, financial-securities clearing, mining and electricity distribution to mobile telecoms, road tolling and weather forecasting also relies on GPS. Among other things, its signals are used to synchronise the clocks in mobile-phone base stations, steer combine harvesters and keep oil platforms in position.

Specialists have been warning for years that this growing dependency is a potential vulnerability. As long ago as 2001 a report from the Volpe Centre, a transport-research body in Cambridge, Massachusetts, described GPS as a tempting target for exploitation by "malicious persons". America's GPS and Russia's GLONASS are currently the only functioning global navigation satellite systems (GNSS), but Europe's Galileo and China's COMPASS systems are under construction.

We're jamming

All of them share a fundamental weakness, however. Because they rely on signals from satellites transmitting from an altitude of around 20,000 kilometres (12,400 miles), the signals are very weak, making them vulnerable to accidental or deliberate interference. This can take the form of natural interference, as a result of solar activity, for example; accidental man-made interference due to signal reflection or faulty transmitter equipment; and deliberate jamming of the satellite signal by transmitters that drown it out by broadcasting their own signal on the same frequency.

British police began finding jamming equipment in the possession of criminals about three years ago. This was not surprising, because evidence from satnavs and vehicle-tracking devices had already been used in several successful prosecutions. In July 2010 two men were jailed for a total of 16 years after they admitted being members of a gang that stole 40 lorries and their loads with a total value of £6m (\$9.6m). They had used GPS jammers to prevent the vehicles being tracked after the thefts. In Germany, meanwhile, some lorry drivers have used jammers to evade the country's GPS-based road-tolling system.

"If you do an internet search on GPS jammers, you get over 300,000 hits, with many of these linking to sites offering them for sale," says Jim Hammond of the intelligent transport systems working group at Britain's Association of Chief Police Officers (ACPO). "I'd suggest you don't get that level of hits for products that nobody buys." ACPO and Britain's communications regulator, Ofcom, are urging the government to make it easier to prosecute people who use and sell jammers, and to make their possession a criminal act.

In November America's National Space-Based PNT Advisory Board said deliberate disruption of GPS was becoming more common, and that the systems in place to find and stop jammers were insufficient. It called for the rapid development of new ways to shut down sources of interference, new laws to punish offenders more harshly and for alternative, non-GPS-based backup systems to be deployed.

In Britain such efforts are already under way. "Efforts to combat interference and jamming have accelerated in the last couple of years in response to a rapid rise in the sale and use of jammers," says David Last, a former president of the Royal Institute of Navigation and a GPS consultant to the British government. The Technology Strategy Board, a body set up to promote innovation, has provided £3m (\$4.8m) in funding for research projects in this field, called GAARDIAN and SENTINEL.

The GAARDIAN consortium, which completes its work this month, has developed equipment to provide real-time information about the reliability of GPS at airports or other sensitive locations using networks of probes. Each probe can pick up GPS signals and signals from eLoran, an enhanced version of Loran, the ground-based terrestrial radio-navigation system first used by the American and British navies during the second world war. The probes also contain a small atomic clock. By comparing the GPS and eLoran time signals with its internal clock, each probe can detect interference and determine whether it is natural or man-made.

The ability to detect man-made interference is not much use unless the source can be located, however. That is where SENTINEL comes in. It is a new research project announced in December by Chronos Technology, the British firm that leads the GAARDIAN consortium. The idea is to use

probes similar to those used in GAARDIAN, but interconnected in such a way that the position of a jamming device can be determined by triangulation. "If there is a power loss on one probe, and weaker power losses in other probes, that could help us pinpoint the source of the problem," says Andy Proctor of Chronos.

In America there is already a military system to spot GPS interference: the GPS Jammer Detection and Location (JLOC) system run by the National Geospatial Intelligence Agency. According to Navsys, the company that developed JLOC, it involves a network of GPS receivers capable of detecting regions of higher than normal signal levels and low signal-to-noise ratios, either of which can indicate interference. But it is unknown how many sensors there are in the JLOC system, or how accurately it can determine the location of a jammer.



Some experts in the field are sceptical that it will be possible to develop cost-effective systems to locate low-power, short-range jammers around civilian infrastructure. It would require a very dense network of sensors, says Dr Last. "I suspect we have reached the stage where close to any major highway you cannot expect to operate a high-availability GPS system without it failing from time to time," he says.

At a GNSS conference in Portland, Oregon, last September, Phil Ward, president of Navward GPS Consulting in Dallas, Texas, proposed an elegant solution. Even low-power jammers could be detected, he suggested, if legislation was passed requiring smartphones, many of which now contain GPS receivers, to look out for jammers and warn other phones nearby if one is detected. The phones would then collectively determine the jammer's location and report it. It is a clever idea, but it would take years to implement.

Navsys may have found a way to speed up the process, however. It says it has received encouraging feedback from America's Defence Advanced Research Projects Agency (DARPA) in response to a recent proposal to develop an app that would turn smartphones running Google's Android software into JLOC sensors. Members of the emergency services, or even members of the public, would then be asked to download the app and leave it running on their phones. This could provide the high-density detection network necessary to locate small jammers.

A down-to-earth alternative

Another way to cope with jammers is to deploy backup systems that do not depend on satellite signals, but rely on terrestrial signals instead. In America radio-navigation and air-traffic-control systems based on terrestrial beacons, which predate GPS, were supposed to be phased out by 2018 in favour of satellite-based alternatives, under a modernisation programme called NextGen, overseen by the Federal Aviation Administration (FAA). Switching to satellite-based air-traffic

control would, for example, allow more direct routes and save fuel, because aircraft would no longer have to follow a wiggly route from one ground-based beacon to another.

In a paper presented at the NAV10 conference in London in December, Mitch Narins, chief systems engineer at the FAA, and colleagues described the Newark jamming incident as “a valuable lesson” because it highlighted the risks of becoming too dependent on satellite-based systems that were vulnerable to disruption. Mr Narins and his team are now investigating whether the old-style terrestrial systems can be modernised and extended to provide a backup that could take over in the event of GPS failures. They expect to make their recommendations in 2013 or 2014, in time for implementation to begin in 2016.

Elsewhere, eLoran is another non-satellite-based alternative which has many cheerleaders. It is an enhanced version of Loran-C, which is itself an improved version of the original Loran (“long-range navigation”) system developed in the 1940s. Once widely used in America, Japan and parts of Europe, Loran fell out of favour with the emergence of satellite-based systems. But its proponents have continued to develop the technology, and eLoran is now accurate to within 10 metres or so, which is comparable to GPS. “It is terrestrial as opposed to spaced-based, uses very high-powered signals rather than low-powered ones and it’s very low frequency instead of high,” says Sally Basker, president of the International Loran Association. “All of which means its failure mechanisms are different to GPS and other satellite-navigation systems.”

Enthusiasm for eLoran is strongest in Britain, where the government awarded a 15-year contract in 2007 to develop eLoran for use by shipping in western Europe. A ministerial decision to move from the development to the operational phase is expected shortly. In the United States and Canada, however, Loran-C transmitters were switched off last year. After a long debate about the merits of keeping the system going, Barack Obama declared it outdated. The House of Representatives has given the Department of Homeland Security until April to decide whether a single, national GPS backup system is required. Which technology would be used to build such a system remains to be seen.

In a way, GPS has become a victim of its own success. Because it is used for such a wide range of civilian purposes, when somebody wishes to disable one GPS-based system, their actions can also disrupt other, unrelated systems. The benefits of satellite positioning are undeniable, and they are only likely to increase in future. But it is now clear that fully realising those benefits depends on putting systems in place to mitigate against deliberate and accidental interference, and to provide an independent backup that does not rely on the delicate trilling of distant satellites.

from the print edition | Technology Quarterly

[About *The Economist* online](#) [About *The Economist*](#) [Media directory](#) [Staff books](#) [Career opportunities](#) [Contact us](#) [Subscribe](#)

[\[+\] Site feedback](#)

Copyright © The Economist Newspaper Limited 2011. All rights reserved. [Advertising info](#) [Legal disclaimer](#) [Accessibility](#) [Privacy policy](#) [Terms of use](#)

[Help](#)

