GPS chaos How a $30 box can jam your life

- by **David Hambling**

Signals from GPS satellites now help you to call your mother, power your home, and even land your plane – but a cheap plastic box can jam it all

IT WAS just after midday in San Diego, California, when the disruption started. In the tower at the airport, air-traffic controllers peered at their monitors only to find that their system for tracking incoming planes was malfunctioning. At the Naval Medical Center, emergency pagers used for summoning doctors stopped working. Chaos threatened in the busy harbour, too, after the traffic-management system used for guiding boats failed. On the streets, people reaching for their cellphones found they had no signal and bank customers trying to withdraw cash from local ATMs were refused. Problems persisted for another 2 hours.

It took three days to find an explanation for this mysterious event in January 2007. Two navy ships in the San Diego harbour had been conducting a training exercise. To test procedures when communications were lost, technicians jammed radio signals. Unwittingly, they also blocked radio signals from GPS satellites across a swathe of the city.

Why would a GPS outage cause such disruption? These satellite signals now do a lot more than inform your car's satnav. GPS has become an "invisible utility" that we rely on without realising. Cellphone companies use GPS time signals to coordinate how your phone talks to their towers. Energy suppliers turn to GPS for synchronising electricity grids when connecting them together. And banks and stock exchanges use the satellites for time-stamps that prevent fraud. Meanwhile, our societies' reliance on GPS navigation is growing by the year.

Some are worried that we are now leaning too heavily on a technology that can all too easily fail – and it doesn't need a freak navy training exercise to cause havoc. Their biggest concern is a GPS jammer – a plastic device that can sit on car dashboards. These can be bought on the internet, and tend to be used by say, truckers who don't want their bosses to know where they are. Their increasing use has already caused problems at airports and blocked cellphone coverage in several cities. One jammer can take out GPS from several kilometres away, if unobstructed. No surprise, then, that researchers across the world are scrambling to find ways to prevent disastrous GPS outages happening.

Weak signal

GPS works thanks to radio signals from satellites. The dominant provider is still the US military's NavStar network, with at least 24 satellites operating at any given time, positioned so that you can always see four of them from anywhere on the planet's surface.

Each satellite continually broadcasts its location and the time as measured by its on-board atomic clock. A GPS receiver compares the time with its own clock, and then calculates how far it must be from each satellite. Once it locks on to at least four satellites and has accounted for errors, it will discover its precise location (see graphic). Nowadays, many receivers also use GPS for cheap and convenient access to the accurate time given by the satellites' clocks.

"The problem is that the GPS signal is very weak. It's like a car headlight 20,000 kilometres away," says consultant David Last, former president of the UK's Royal Institute of Navigation. You can't boost the signal any further because of the limited power supply on a satellite.

Last has first-hand experience of how easy it is to block a GPS signal, and the effects it can have on modern technology. In 2010, he conducted an experiment in the North Sea, aboard the THV Galatea, a 500-tonne ship. The Galatea is the pride of its fleet, with all the latest navigation equipment. Last wanted to find out how it would cope without GPS. So he used a simple jamming device that overwhelmed the GPS signal by broadcasting noise on the same frequency as the satellites.

When Last activated the jammer, the ship went haywire. According to the electronic display on the ship's bridge, the Galatea was suddenly flying at Mach speeds over northern Europe and Ireland. Then alarms sounded. The ship's navigation backup – its gyrocompass – crashed, because it uses GPS to provide corrections. The radar did the same. Even the ship's satellite communications failed, because GPS points the antenna in the right direction. "The crew were well trained and briefed, so they knew what was going on," says Last. "But, like us, they were surprised."

Truck cheats

Last deliberately simulated a simple, commercially available jammer. Though illegal to use in the US, UK and many other countries, these low-tech devices can be bought on the internet for as little as $30. Sellers claim they're for protecting privacy. Since they can block devices that record a vehicle's movements, they're popular with truck drivers who don't want an electronic spy in their cabs. They can also block GPS-based road tolls that are levied via an on-board receiver. Some criminals use them to beat trackers inside stolen cargo. "We originally expected that jammers might be assembled by spotty youths in their bedrooms," says Last. "But now they're made in factories in China."

Last is worried that jammers could cause as much havoc on land as he discovered on the Galatea, and he's not alone. In November 2010, a NASA-appointed executive committee for "space-based positioning, navigation and timing" warned that jamming devices could cause disaster if activated in cities. It is not known how many are out there, but the panel is concerned that the risk of interference is growing fast. And in future, devices called "spoofers" – which subtly trick GPS receivers into giving false readings – may make the problem even worse (see "Faking it").

An event last year at Newark Liberty International Airport in New Jersey showed that it only takes one jammer to cause disruption. Airport controllers had installed a new GPS-based landing system, so that aircraft could approach in bad visibility. But it was shutting itself down once or twice a day. It took several

months to find the culprit: a driver on the nearby New Jersey Turnpike using a portable GPS jammer to avoid paying the highway toll. This trucker was cruising past twice a day, crippling an airport as he went.

Future generations of air-traffic control won't work without GPS – nor will train routing. The US Federal Railroad Administration has GPS at the heart of its plan for smart management of rail traffic. GPS is also increasingly relied upon for guiding emergency services to the scene.

Invisible utility

What's more, a lot more than navigation ability is lost when GPS fails today. "We rely upon GPS without even being aware of it," says Donald Jewell, who helped to establish GPS from its inception in the US air force, and is now editor of *GPS World* magazine. It is estimated that more that a billion GPS receivers are now in operation, he says, and more than 90 per cent use the signals only for the accurate time provided by the satellites.

Cellphones are a key user of this invisible utility. Towers must synchronise with each other to pass calls to other towers as you move – a GPS time signal offers a cheap and accurate way to do this. The timing offset for each tower is also used to identify it. In fact, many wireless communication technologies use GPS timing for synchronisation. That's probably why the harbour traffic control and emergency pagers failed in San Diego in 2007.

Time is money

GPS timing can time-stamp financial transactions, such as stock-market trading. And ATMs sometimes communicate wirelessly, using a time-based encrypted code that requires synchronisation. Though it is not known why the cash machines stopped working during the San Diego event, this might have something to do with it.

Energy suppliers use GPS time to keep alternating current from various power plants in phase across the grid. If frequency cycles are not matched, two supplies will partially cancel each other out, creating inefficiency. A precise time signal allows operators to pinpoint the start of each cycle. The US power grid, for instance, requires synchronisation between the supplies of over 5000 companies. Yet in 2006, a temporary GPS outage due to sunspot activity meant that energy companies were not able to see where the power was going, which resulted in false billing. Blackouts due to GPS failure are not out of the question.

Given the potential for disruption, law-enforcers are trying to crack down on GPS jamming. In February, the US Federal Communications Commission announced a new effort to fine jammer sellers and owners. The problem for western authorities is that most sellers are in east Asia and laws tend only to cover the use of a jammer, not its ownership.

Safety net

That's part of the reason why navigation researchers are calling for a back-up. To discuss what to do next, many of them will gather for a meeting next week at the National Physical Laboratory in Teddington, UK.

Fortunately, there's a backup right under our noses, and the idea been around since the 1940s. Just like GPS, it provides navigation and accurate timing. It's called Enhanced LORAN (eLORAN).

Basic LORAN (for long range navigation) is similar to GPS but uses ground-based radio signals rather than from satellites. It doesn't have global coverage, but does beat GPS on some things. LORAN operates at a far longer wavelength than GPS signals and is more powerful. Both of these features make it virtually impossible to jam.

A new version, eLORAN, uses more reliable transmitters and features improved caesium atomic clocks. With software modifications, it is accurate to about 10 metres, as well as providing a time signal of similar accuracy to GPS. It would be easy to modify future receivers to switch over to eLORAN without the user even noticing, says Last.

In Europe, a team at the UK's General Lighthouse Authorities has been testing eLORAN, and is now recommending that the UK government rolls it out. Across the Atlantic, however, the US government is taking its current LORAN out of service. And it has so far rejected all advice to fund eLORAN: which would cost about $20 million per year – less than it costs to launch one GPS satellite. "We still hold out hope that someone with some foresight and technical know-how in our government will see the light," says Jewell.

Happily, a few decades from now a GPS signal might not be required at all for many things. If atomic clocks get cheaper, then they could be built into everything that needs accurate time. And eventually you'll be able to navigate without any external signals, thanks to devices called "inertial measurement units", which track your movements from a known start point. Today, these IMUs use gyroscopes to measure orientation, plus accelerometers to tell how fast it is accelerating. Using this information, plus time, the acceleration is converted into speed and distance to reveal relative location.

Today, IMUs drift about 1.5 kilometres per hour of travel, and are large and expensive. Yet the US Defense Advanced Research Projects Agency plans to improve performance with a microchip-sized atomic clock and an equally diminutive, accurate acceleration sensor.

In the meantime, however, a generation is growing up that has never known life without GPS. As jammers proliferate, GPS outages like San Diego are likely to become more common. So next time you lose your cellphone signal, blame the little black box on a car dashboard a few kilometres away.

Get there in a flash

Your satnav might one day find its route thanks to the faint flashes of distant lightning.

Both GPS and LORAN (see main story, above) are navigation techniques that rely on radio signals to pinpoint your location, but these signals can't penetrate underground or deep inside buildings.

Now the US Defense Advanced Research Projects Agency (DARPA) is testing the idea of using radio pulses from lightning instead. These natural atmospheric radio sources – or "sferics" – have a very low frequency, so can penetrate deep underground and even underwater. The military is interested because it would improve navigation in caves and tunnels or for submarines.

DARPA's S-BUG receivers detect radio waves emitted by lightning thousands of kilometres away – at any given moment there are around 2000 storms active on the planet. Another device feeds the receiver the exact location and emission time of the sferic so that it can calculate how far away it is. Once several sferics are recorded, the receiver can then use this to discover its location.

DARPA is still testing S-BUG. But once a lightning receiver network is fully in place, existing GPS users should require nothing more than an antenna and a software upgrade to use the system, says programme manager Stephanie Tomkins.

Faking it

Todd Humphreys can trick you into thinking you are somewhere else. He uses a "spoofer" device that causes a GPS receiver to give an inaccurate reading.

Humphreys, at the University of Texas at Austin, has no mischief in mind, but built the device to demonstrate how straightforward it is to do. Such spoofers are not on the market yet, but when they are, could cause all sorts of havoc.

Unlike a GPS jammer, which has fairly obvious effects, the spoofer's impact is slow and subtle. "The victim usually won't realise they're being spoofed," says Humphreys. "It leaves no trace."

Humphrey's GPS spoofer looks like a wireless internet router. It picks up genuine GPS signals and synchronises its output to resemble them. Any nearby receiver will treat this output as a genuine signal from a GPS satellite. The spoofer then gradually alters its time output, changing from the true value by, say, 3 nanoseconds per second. Since GPS receivers use the time signature in a signal to find location or as an easily accessible clock, the error builds up.

"The biggest risk is probably complicit spoofing, where someone deliberately misleads their own GPS," says Humphreys. For example, unscrupulous fishing boat captains could spoof GPS to fake their location and fish in forbidden waters. "If mass-produced, they could be made for perhaps $400 to $500," says Humphreys. Such a spoofer could push another ship off course, just as ship-wreckers used to lure vessels onto rocks with false lighthouse lights.

Criminals could also spoof GPS timing for profit. The US National Association of Securities Dealers requires financial traders to time-stamp transactions with an accuracy of within 3 seconds. "The bad

guys would spoof the timing at their preferred site and, watching an upward trend, buy stock a few seconds in arrears," says Humpreys. "Those three seconds could be worth a lot of money."

David Hambling *is a writer based in London*