Signal Disruptions

GNSS… it's almost impossible to run a modern geo-related business without it. But what if a problem should occur? Whether in navigation, surveying or even agriculture, countless activities almost entirely depend on GNSS. As long ago as 2001, the US Volpe report warned users about the potential impact of GNSS issues.

For many years, the eLoran system – the updated version of Loran-C – was suggested as the best alternative to GNSS. And maybe it is… or rather was, since governments around the world have increasingly lost faith in it since Barack Obama declared Loran obsolete for the USA in 2009. European governments stopped providing funding and retired their eLoran programmes around 2016. As a result, GNSS is now Europe's only navigation system – if you accept that four strictly separate systems utilizing the same technology and frequency bands can be considered a single system, that is.

So what is all the fuss about? Well, ever since the start of GPS, the system has been easy to disrupt. One type of disruption are the outages experienced due to the increase in magnetic activity during a solar storm, causing GNSS signals to become unstable or lost. However, most disruptions are man-made. It all started with the Americans themselves who decided to degrade the signals using selective availability (SA). In 2000, when Bill Clinton discontinued SA and promised never to turn it back on, selective deniability was stressed as a potential option to deny GPS signals over a certain area – so in effect a 'controlled' disruption.

But governments are not the only ones who can disrupt GNSS services. Every 'hacker' has a number of options within easy reach. The simplest form, jamming, locally blocks out all signals for specific frequencies, and even a very small transmitter can be enough to deny GNSS access over a substantial area. This is possible because satellite signals are weaker than not only other signals in general but also than the background 'noise'. On the bright side, because jamming means that everything suddenly stops working, at least it's immediately obvious that there's an issue.

Spoofing is a much more sophisticated form of disruption involving the transmission of false ('spoofed') signals that appear to be genuine ones. Since the spoofed signals are stronger, they 'overrule' the original satellite signal. Receivers locking on to these signals can be fooled into thinking they are elsewhere. This technique is relatively easy to implement yet much harder to detect. And as you can read elsewhere in this edition, even some gamers have started using this technology so that they can stay in the comfort of their own homes rather than having to go outside.

Over the years, both jamming and spoofing have become ever-more serious problems for serious applications. Most gamers probably aren't even aware of the fact that their spoofing activities could disrupt satellite navigation systems in cars, for instance. Attentive drivers are likely to notice such a problem immediately, but what are the implications for autonomous driving? Do we have backup systems in place or is GNSS our sole means of positioning?

The good news is that the designers of GNSS and also the receiver manufacturers are aware of these issues. Solutions are being implemented in receivers themselves to enable them to discriminate between genuine and false signals. More importantly, new signal-related developments will allow receivers to authenticate that a signal is actually coming from a satellite rather than a hacker on the ground. This will help to prevent spoofing – at least until hackers find a new way of disrupting GNSS services…

New signal-related developments will allow receivers to authenticate that a signal is actually coming from a satellite rather than a hacker on the ground. This will help to prevent spoofing.