Photo: Oleksandr Kalinichenko / Shutterstock.com

GNSS: are you on the right track?

Guy Buesnel surveys the threats to satellite navigation signals, reviews the ways in which they can be mitigated, and looks at the prospects for industry-agreed standards

Nearly 70 years ago, the first artificial satellite was launched, and by 2012 there were 1,000 satellites orbiting the earth. Today, Global Navigation Satellite System (GNSS) technology and the Global Positioning Systems (GPS) receivers with which they communicate are commonplace.

The technology's precision and universal availability makes it ideal for a variety of uses, from fleet management to asset protection. But it is also a prime target for cyber attackers using RF interference, jamming and the deliberate counterfeiting of signals known as spoofing. But there are a number of ways in which to mitigate the risks, using routine assessments and tests, leveraging commercial laboratory test beds, and establishing international, industry-wide standards.

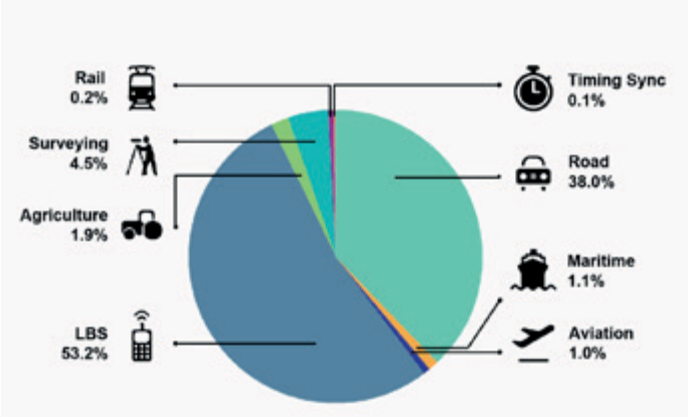
According to a market study by Navipedia[1] (an initiative of the European Space Agency that serves as a source of general knowledge on GNSS topics), the global installed base of GNSS devices is estimated at 3.6 billion units ... a figure that is expected to climb to seven billion by 2019. GNSS is already used by critical infrastructure organisations such as utility providers, as well as by the financial and transport sectors to provide timing or positional data, and growth in emerging markets such as the Intelligent Transport sector will see GNSS data exploited for safety-critical applications.

The Navipedia study indicates that smartphones continue to be the predominate types of devices using GNSS technology, (3.08 billion in 2014), followed by devices for road applications (0.26 billion). Other GNSS-enabled devices include those employed by aviation, rail, maritime, agriculture, surveying, timing and synching.

Growing concerns

There are growing concerns that jamming, and spoofing signals that can interfere with, or even take over GPS systems pose serious threats. In an InfoSec Institute report[2] that detail the various security threats to satellite systems, jamming and GPS spoofing are listed as two of the top 10 threats.

Jamming is performed by transmitters emitting electromagnetic interference that blocks the reception of GPS broadcast signals. According to an October 2014 notice from the U.S. Federal Bureau of Investigation's cyber division[3], auto thieves sending stolen vehicles to China used GPS jammers to thwart tracking of the shipping contain-



Cumulative core revenue 2013-2023, GNSS Market Report 2015.
Graphic: European GNSS Agency (GSA)

ers. Cargo thieves in North Florida used GPS jammers to prevent tracking of a stolen refrigerated trailer. Or consider the trucker who decided to conceal his whereabouts and drive beyond his legal maximum number of hours by using a GPS jammer. It's a true story; fortunately the trucker was caught because his GPS jammer inadvertently jammed a nearby cell tower.

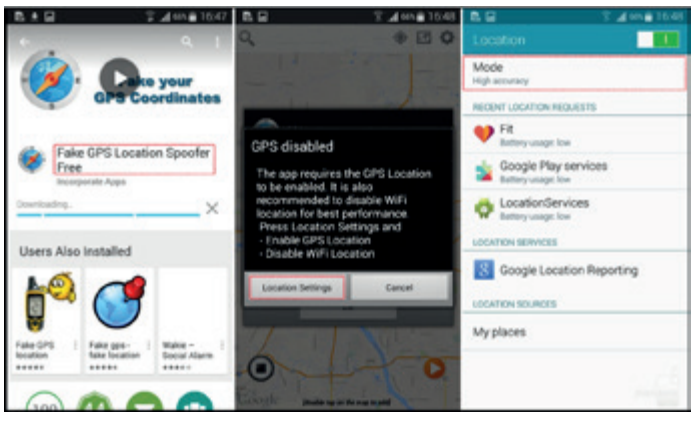
There are also inexpensive apps for tablets and smartphones that can be downloaded (after jailbreaking the operating system) that allow users to spoof a device's location. While such apps can't fake GPS signals, they can manipulating the data supplied to applications on phones or tablets that require GPS position data.

Insidious threat

To fake a GPS signal, a spoofing device interferes with a GPS receiver and tricks it into tracking counterfeit GPS signals. The InfoSec Institute report says GPS spoofing is one of the most insidious threats to GPS systems. The false GPS signals can fool receivers into thinking they are at a different location and could be used in the hijacking of drone or a vessel. However, effective spoofing devices are neither cheap nor easy to deploy, requiring more than a simple app to generate signals that are not immediately recognised as spurious.

For example, in 2013 a radio navigation research team from the University of Texas was able to coerce a 213-foot yacht off course using a custom-made GPS device (that reportedly cost $3,000 to make). The team had to board the yacht, by the way, and had the cooperation of the captain and crew. The researchers were this year invited by the U.S. Department of Homeland Security to perform a follow-up test by faking navigational signals to a GPS-guided vehicle.[4]

Spoofing signals that guide ships or drones is of concern, but equally alarming is the growing reliance of everything - from power grids to financial trading systems - on precise timing data from navigation satellites. For example, every cell tower has its own GPS receiver to provide a super-accurate time signal for its own transmis-



Smartphone apps manipulate GPS data to spoof a device's location

High-speed money market trading systems rely on GPS timing data to time-stamp trades. *Photo:* Tenaclousme (Creative Commons License Attribution 2.0)

sion purposes. And some financial high-speed trading systems are so time critical that they rely on GPS time data to determine precisely when trades were made. My view is that we are likely to see GPS spoofing emerging as a new form of critical infrastructure hacking. Imagine the potential impact of hacking a power network using GPS time spoofing, whether the effect is to alter or disrupt the flow of electricity, or even to mask abnormal activity on the grid.

Outsmarting the jammers and spoofers

There are, of course, some obvious ways to detect if a ship is being spoofed onto an unwanted track. Apart from visually detecting an unplanned change of direction, GPS can be augmented with alternative positioning systems such as those that employ dead-reckoning or by an alternative position-fixing system such as eLORAN. Also of help would be the availability of a secondary multi-constellation, multi-frequency GNSS receiver.

Organisations should also routinely assess and test their GPS equipment so they understand how an attack affects their systems

Another alternative to GPS for use in busy waterways is radar. Here, Helmut Lanziner who developed the RadarFix system in the late 1980s, demonstrates Russell Technologies' latest XIR3000 digital radar processor unit. This add-on to contemporary radar transceivers and a further evolution of the RadarFix system works with onshore radar reflectors and other fixed targets to obtain accurate range and bearing measurements. These are superimposed with a radar image overlay on an electronic chart to display a vessel's movement in real-time and to an accuracy of around two meters depending on the number of targets. *Photo: GeoConnexion*

In 2012, a team led by Assistant Professor Todd Humphreys of the Cockrell School of Engineering at the University of Texas (pictured) was the first to successfully demonstrate that the GPS signals received by an unmanned aerial vehicle (UAV), or drone, could be commandeered by an outside source.[4] *Photo: University of Texas at Austin, Department of Aerospace Engineering & Engineering Mechanics*

and how they might respond. Understanding the equipment and its ability to withstand or mitigate an attack is vital. Are their GPS receivers sufficiently robust to resist drive-by jammers? Will they output misleading data? One of the most dangerous effects of GPS jamming is that, as a jammer gets closer, some receivers will start outputting hazardously misleading information, such as incorrect positions or times that could lead to costly mistakes. If a receiver is jammed or spoofed, will it detect the attack and generate an alert?

Risk assessment should also be a priority. How likely is it that jamming would be encountered at a specific site or on a specific fleet? What is the likely frequency of jamming or spoofing events? What would be the impact of such events on the business in terms of lost hours of productivity?

There are also commercial, laboratory test beds emerging that incorporate simulators, monitors and computers with software designed expressly for GNSS testing and which include testing against possible spoofing attacks. These test beds could allow a large GNSS user or receiver manufacturer to establish how well their equipment performs and how vulnerable it is to attack. Similarly, such test beds enable device manufacturers to develop standardised tests against set criteria to improve the performance and reduce the vulnerability of their products.

Interference simulation systems, such as Spirent's GSS7765, are used to test satellite navigation equipment in the presence of intentional or unintentional RF interference. *Photo: Spirent Communications*

The SimSAFE software tool, jointly developed by Spirent and Qascom and unveiled at the end of last year, represents an innovative approach to the laboratory simulation of GNSS attacks and the testing of receiver mitigation techniques *Image: Spirent Communications*

'My view is that we are likely to see GPS spoofing emerging as a new form of critical infrastructure hacking'

There may eventually be industry-accepted criteria that will help users select the best GNSS equipment for their chosen applications based on its level of protection against jamming and spoofing. But one thing's for sure: It isn't likely we'll see openly-published industry standards for GNSS test beds any time soon. That would be a gift to hackers!

References

1. http://www.navipedia.net/index.php/GNSS_Market_Report#Report_Overview
2. http://resources.infosecinstitute.com/hacking-satellite-look-up-to-the-sky/
3. https://info.publicintelligence.net/FBI-CargoThievesGPS.pdf
4. http://www.ae.utexas.edu/news/features/todd-humphreys-research-team-demonstrates-first-successful-gps-spoofing-of-uav

Guy Buesnel is Product Manager for the Positioning & Navigation Business Unit at Spirent Communications plc (www.spirent.com)