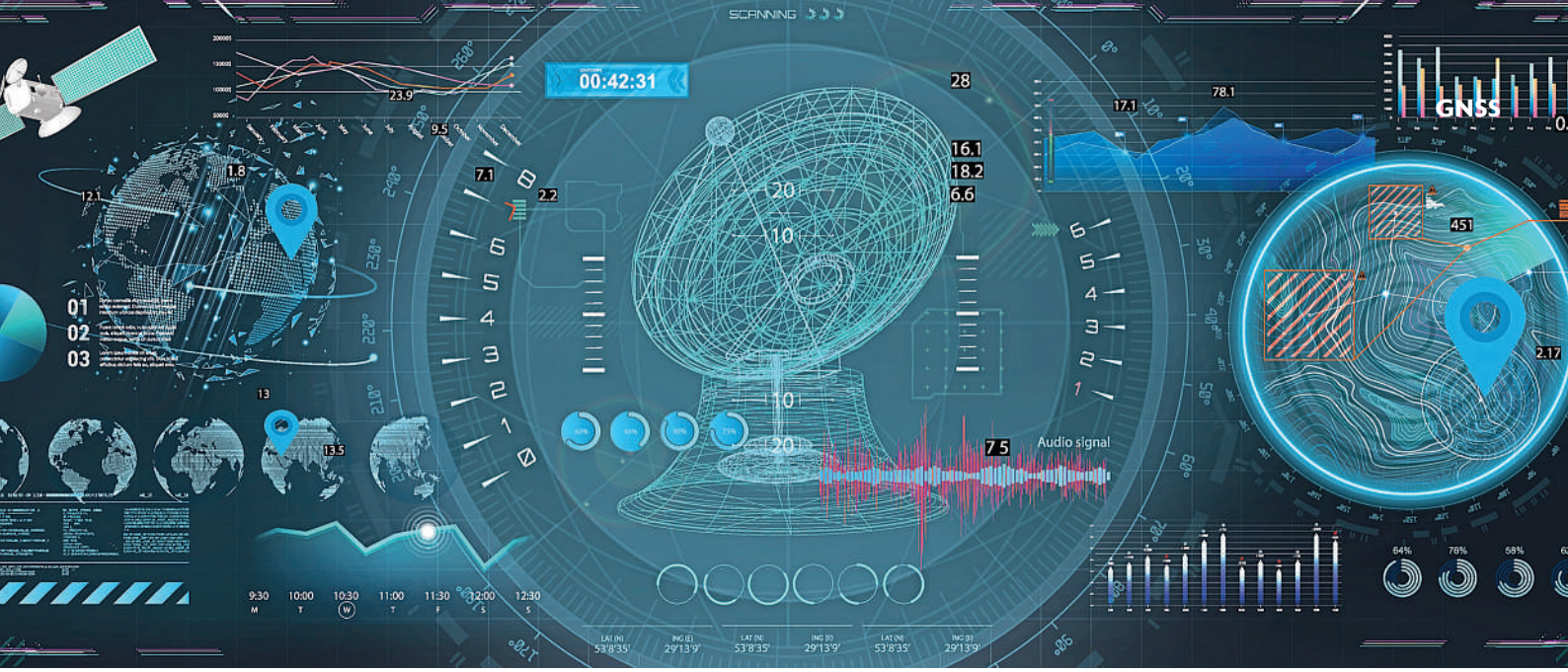
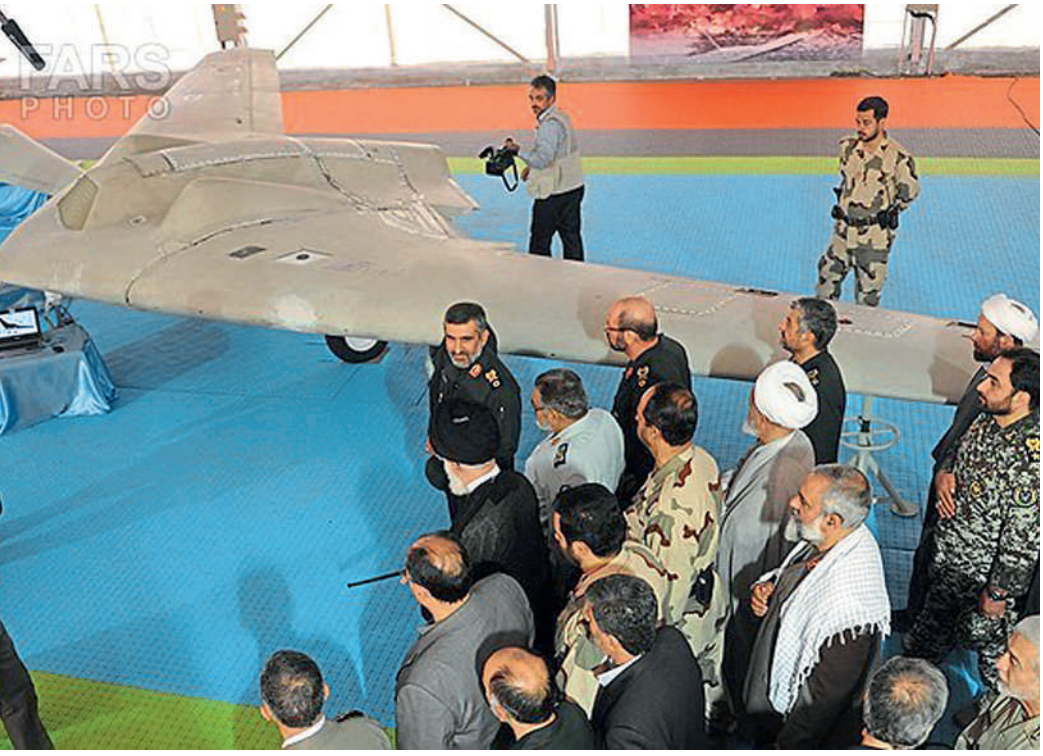


HIDE AND SEEK: THE THREATS TO GNSS

THE ABILITY TO SPOOF, HACK, OR JUST PLAIN CONFUSE GLOBAL NAVIGATION SATELLITE SYSTEMS (GNSS) HAS BEEN AN ISSUE SINCE THE EARLY 1990s, **GUY BUESNEL** BRINGS US UP-TO-DATE BY REPORTING ON THE LATEST THREATS AND COUNTERMEASURES



In 2011, the Iranian government announced that this American Sentinel UAV was commandeered by its cyberwarfare unit and safely landed near the city of Kashmar. One speculation is that both satellite and land-originated control signals to the UAV were jammed and followed by a GPS spoofing attack that fed the UAV false GPS data to make it land in Iran rather than what the drone thought was its home base in Afghanistan. Photo: Fars Media Corporation, CC BY 4.0, https://commons.wikimedia.org/w/index.php?curid=72669030

Whether it's a high-profile incident such as in December 2011 when Iran reported it had captured a US "Sentinel" stealth drone through alleged spoofing. Or mass events such as the two dozen ships operating in the Black Sea in June 2017 where on-board GPS placed them at airports many miles from their actual location. To recent incidents such as nine "ghost ships" that appeared to be circling off the coast of San Francisco during 2020 due to seemingly false GPS signals – although some experts believe it might have been due to a weird fault.

Many of the challenges are often faced by shipping, and in recent years, the scale and scope of the problem prompted the US Department of Transportation Maritime Administration to issue a formal warning in October 2021.

Type of attack

Spoofing is a very broad term for an attack focused on fooling a user into thinking that information they are receiving is true when in fact it is false. These generally fall within five categories, namely:

Meaconing is the delayed transmission of inauthentic Global Navigation Satellite System (GNSS) signals to a target receiver. If the meaconing attack is successful, the target

receiver will report the position contained in the re-transmitted data rather than the true position. Meaconing can be accidental if devices are not sufficiently isolated.

Code/carrier attack is when an attacker replicates GNSS signals using an RF signal generator. The aim is to align the replica signals, often the whole constellation, to the authentic signals being received by the target receiver and once the receiver's tracking loops are locked onto the replica signals, an attacker can manipulate the fake code and carrier signals to force the target receiver to report an incorrect position.

Navigation data attack is like a code/carrier, but the attacker only adjusts the navigation message content on one or more of the faked signals to produce gross errors in the target receiver or even denial of service. For instance, an attacker could set satellite status to "unhealthy".

Application-level spoofing targets the transmission of data from GNSS receivers to Positioning, Navigation and Timing (PNT) systems through man-in-the-middle type attacks. This can be exploited to force systems to report incorrect time and location data with no need for any of the equipment or techniques associated with RF spoofing attacks.

Multi-method attacks involve a combination of the above methods, and may also use equipment such as antenna arrays, high-powered transmitters and even low earth orbit (LEO) satellites. This kind of attack is usually limited to attackers with significant resources and motivation for electronic warfare.

Combating the threat

Spoofing attacks using RF interference are on the rise as the cost of the equipment needed to carry out assaults has fallen significantly in recent years. New technology such as programmable software defined radios plus the expertise required to carry out a spoofing attack have both become widely available via the internet.

The most concentrated efforts have come from the military with the US and NATO mandating the use of GPS P(Y) code signal encryption as standard. Looking forward, the next generation M-Code standard is designed to give military receivers better protection against jamming using a flexible cryptography architecture with the ability to detect and reject false signals. It provides military users with a dedicated GPS signal separate from the civilian one and is currently under testing.

Civilian efforts include Open Service Navigation Message Authentication (OSNMA), an anti-spoofing service developed for the European GNSS system (Galileo) that is undergoing final testing. OSNMA secures Galileo signals through authentication of navigation and satellite location data using a hybrid symmetric/asymmetric cryptography technique that is designed to be backward-compatible.

These new GNSS signals using hash-type encryption architectures such as OSNMA where receivers can authenticate messages are a significant step forward for GNSS security.

However, it does not eliminate the risk of meaconing. The handling of authenticated signals in a PNT system must also be carefully assessed: for example, if there is a failure of the authentication mechanism at the transmitter, what are the consequences of signal rejection for the system's behaviour and for the end-user? Also, "man in the middle" type attacks or sophisticated multi-method attacks that employ advanced techniques – backed by state level resources - are still a major concern.

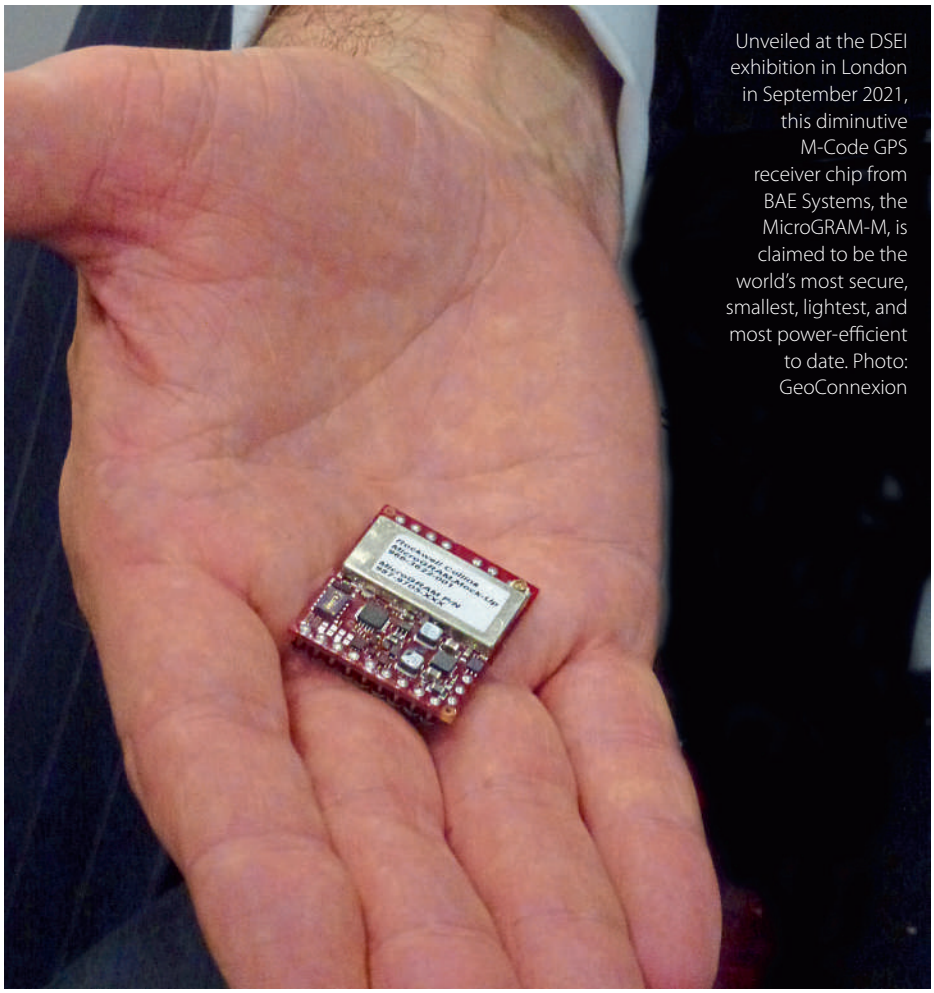
As well as deliberate instances of jamming and spoofing, there are also unintentional interference events that require as much attention as malicious threats. For example, problematic noise in adjacent bands to GPS is also on the rise as governments world-wide sell off spectrum for other applications.

Protect, Toughen and Augment

The problem of spoofing is multi-dimensional, and combatting it requires effort across multiple fronts. As a starting point, a coherent principle such as the 'Protect, Toughen and Augment (PTA)' approach proposed by Dr. Bradford Parkinson should gain wider adoption.

PTA advocates using a layered approach to risk reduction when evaluating the

Above left: The pioneering OSNMA service will pave the way towards robust and freely available Position, Velocity and Time information (PVT) for Galileo Open Service users. Above right: The main Galileo Security Monitoring Centre (GSMC) at St. Germain-en-Laye, near Paris, monitors the operational status of the system and responds to security threats and alerts. Images: ©European Agency for the Space Programme



Unveiled at the DSEI exhibition in London in September 2021, this diminutive M-Code GPS receiver chip from BAE Systems, the MicroGRAM-M, is claimed to be the world's most secure, smallest, lightest, and most power-efficient to date. Photo: GeoConnexion

performance of Positioning, Navigation and Timing solutions. This approach moves away from a critical dependency on GNSS and toward a future that engages other PNT sensors and systems to provide redundancy and higher levels of resilience.

PTA combines improved operational procedures based around PNT data use and system dependencies, toughening of receivers, the use of modern antenna technologies and augmenting GNSS use with another PNT source.

Manufacturers of GPS-dependent systems should test their existing products to understand how they behave in the event of Radio Frequency interference including spoofing, vulnerability of their systems to man-in-the middle type attacks that could be implemented by a hacker, and the security of PNT data.

Risk assessment

From an end user perspective, carrying out a risk assessment should be a high priority. However, this assessment is not a 'one hat fits all process'. The first step should be an assessment of PNT data use and dependencies as well as the risks to the operation if the flow of that PNT data is denied or disrupted. This should include understanding the most important performance parameters of the equipment necessary to meet operational requirements.

For some applications, for example, the timeliness of a position fix may be more important than the accuracy. If the system is providing precision time services, it may be more important to understand how the pulse per second (PPS) behaves under spoofing conditions.

For safety- or liability-critical applications, this analysis should include alarm threshold levels, time to alarm, and the direct and collateral impacts that a spoofing attack could have on the system. A risk assessment and analysis will inform several important testing decisions. Does the antenna need to be tested independently? If so, testing may need to be conducted in an anechoic chamber or even on a live range. If testing is to be conducted in a laboratory environment, will simulated signals be sufficient or will it be necessary to introduce authentic live-sky signals?

A risk assessment plan will often require specialist guidance but the rapid rise in the scale and scope of the problem means that all users need to at least have the conversation about assessment and mitigation strategies. There is no magic bullet. Spoofing of GNSS is unfortunately here to stay–and a "head in the sand" approach to dealing with its impact is not a viable option.

Guy Buesnel is a PNT Security Technologist with Spirent Communications headquartered in Crawley, West Sussex (https://www.spirent.com)