CASE STUDY

Testing times: How badly are drones affected by GNSS spoofing?

The Bundeswehr Technical and Airworthiness Centre for Aircraft (WTD-61) is attempting to find out using a Spirent mobile GNSS simulation platform.

Spirent™ | WTD-61

CASE STUDY

Testing times

How badly are drones affected by GNSS spoofing?

The Bundeswehr Technical and Airworthiness Centre for Aircraft (WTD-61) is attempting to find out using a Spirent mobile GNSS simulation platform.

Background

Accurate and reliable positioning, navigation and timing (PNT) systems powered by global navigation satellite systems (GNSS) are a necessity for the effective operation of all manner of vehicles. Everything from the millions of trucks delivering goods via our roads to fully autonomous camera drones used in the filming of the latest Hollywood blockbuster; accurate positioning information is vital for both efficiency and safety.

With the growing use of unmanned aircraft systems (UAS), which usually comprises a "drone" aircraft, the control station and the communication link between the control station and the aircraft, inaccurate GNSS information leading to UAS crashes or other incidents such as accidentally entering restricted airspace is a real danger. In addition, recent malicious attacks such as drones buzzing around major airports have caused safety concerns, massive delays and financial penalties. These factors are prompting research to aid in protection of legitimate UAS users from disruption - as well as for methods of potentially disrupting the operation of malicious UAS in restricted airspace.

spirent

Challenge

WTD-61 Studies GNSS Spoofing to Disrupt UAS

The Bundeswehr Technical and Airworthiness Centre for Aircraft (WTD-61), a German Armed Forces test centre specialising in the evaluation of military aircraft and aerial weapon systems, began a test project to evaluate how vulnerable a range of commercial UAS are to GNSS spoofing. In its most understood form, spoofing is the act of broadcasting a fake GNSS signal at a higher power than the genuine signal, to force a GNSS receiver to lock on to the fake signal. This can then be used to manipulate its calculated position or trajectory to any number of ends – including theft, disruption, and even terrorism.

WTD-61 is primarily tasked with the testing of airborne equipment developed by industry on behalf of the Bundeswehr to ensure that only safe and high-performance equipment is being used in operation. This includes WTD-61 being the German national competence centre for UAS. As part of this scope, WTD-61 worked with technical experts from the Fraunhofer IIS using Spirent test equipment to power spoofed GNSS signals at an open-air test range in a remote location, secured so as not to interfere with other civilian or civil equipment.

GNSS spoofing with Spirent's mobile simulator

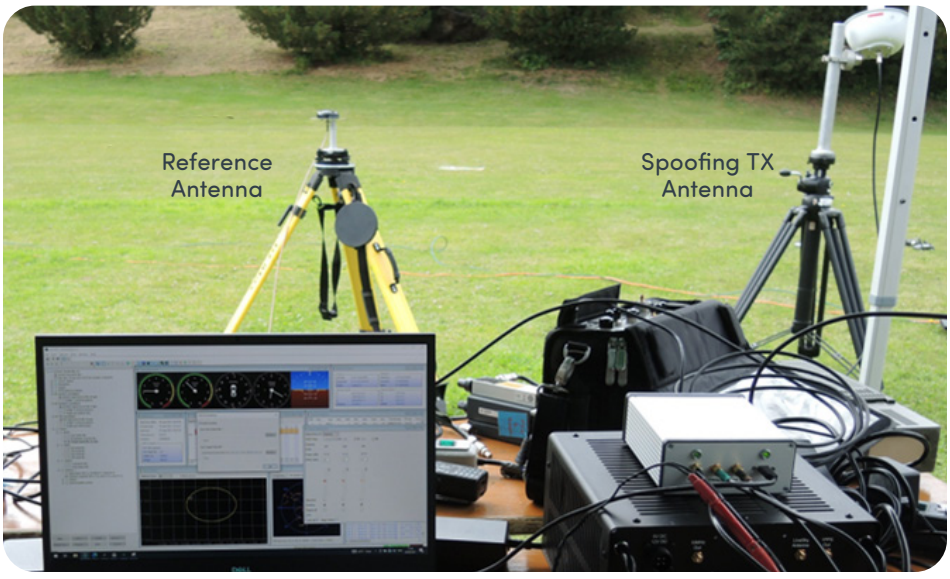
The Spirent mobile GNSS simulation platform is a custom-built unit designed specifically for these types of specialist scenarios. The unit is based on the commercially available, top-of-the-line Spirent simulation engine and supports multi-frequency, multi-GNSS applications with highly flexible configurations. The portable unit also uses Spirent's live sky synchronisation tool, Standpoint, to facilitate over-the-air (OTA) testing in live sky conditions. This enabled the simulator to synchronise the GNSS signals it generates to the satellite signals being received by the UAS under test. In the specific case tested by WTD-61, the Spirent mobile platform emitted signals through a locally connected antenna broadcasting Galileo E1, GPS L1, and GLONASS G1 signals. The test defined the target power at the device under test (DUT) to -90 dBm – significantly louder than the live GNSS signals, to mimic a common over-the-air PNT takeover technique. The test setup compensated for free space loss encountered in OTA testing by employing a high gain broadcast antenna and an external gain block as well as leveraging the high-power output of the Spirent simulator.

Researchers from WTD-61 then evaluated the effects of spoofed GNSS signals for 8 of the most common commercial UAS from well-known manufacturers including DJI and Parrot. These ranged from a 300g consumer model controlled via a smart phone all the way through to a 4.5kg UAV typically used for professional filmmaking. Using Spirent's Standpoint, the test initially tightly synchronised the simulator with the live sky signals. Then the test broadcasted 10 seconds of aligned static positioning data to trick the UAS positioning engine into prioritising the more powerful spoofed signals.

Once the UAS was locked onto the spoofed signal, the researchers then ran through a test process where modified GNSS signals were broadcast to tell the UAS that the drone is drifting at an accelerating rate away from its intended hovering position. In most of the UAS under test, the onboard systems designed to maintain a hover at a fixed position would instead accelerate back to compensate the spoofed location. This behaviour was repeatable over multiple tests and although each UAV test had an experienced pilot ready to take over, many of the drones reacted unexpectedly in terms of changes in direction and altitude.

UAS Vulnerability to GNSS Spoofing: Test Results

Some of the UAS under test are known to have additional sensors and complementary positioning technologies to aid against attacks such as spoofing. However, every UAS under test displayed or reported unexpected behaviour, suggesting a level of susceptibility that could be exploited. The test also conclusively demonstrated that it would be feasible to consistently manipulate a UAS position solely by spoofing the GNSS receiver. A final take away from the project is that without effective testing against the range of threats a UAS might encounter, the possibility of flying BVLOS (beyond visual line of sight), or even wholly autonomously, still has significant risks.



Test setup including Spirent's mobile simulator and Standpoint

Unexpected behavior exhibited by a device under test

Americas Europe Asia

About Spirent Positioning Technology

Spirent enables innovation and development in the GNSS (global navigation satellite system) and additional PNT (positioning, navigation and timing) technologies that are increasingly influencing our lives.

Our clients promise superior performance to their customers. By providing comprehensive and tailored test and assurance solutions, Spirent assures that our clients fulfil that promise.

Why Spirent?

Over five decades Spirent has brought unrivalled power, control and precision to positioning, navigation and timing technology. Spirent is trusted by the leading developers across all segments to consult and deliver on innovative solutions, using the highest quality dedicated hardware and the most flexible and intuitive software on the market.

Spirent delivers

- Ground-breaking features proven to perform
- Flexible and customisable SDR technology for future-proofed test capabilities
- World-leading innovation, redefining industry expectations
- First-to-market with new signals and ICDs
- Signals built from first principles — giving the reliable and precise truth data you need
- Unrivalled investment in customer-focused R&D
- A global customer support network with established experts

ilac-MRA A2LA ACCREDITED | ADVANCED CERTIFICATION 8872 UKAS | INVESTORS IN PEOPLE Platinum Until 2022

About Spirent Communications
Spirent Communications (LSE: SPT) is a global leader with deep expertise and decades of experience in testing, assurance, analytics and security, serving developers, service providers, and enterprise networks. We help bring clarity to increasingly complex technological and business challenges. Spirent's customers have made a promise to their customers to deliver superior performance. Spirent assures that those promises are fulfilled. For more information visit: **www.spirent.com**

Americas 1-800-SPIRENT
+1-800-774-7368 | sales@spirent.com

Europe and the Middle East
+44 (0) 1293 767979 | emeainfo@spirent.com

Asia and the Pacific
+86-10-8518-2539 | salesasia@spirent.com

MCD00471 Issue 1-00 | 10/22

spirent™