THE SPOOFING THREAT

THERE HAS BEEN A HUGE INCREASE IN UAVS BEING USED TO CARRY OUT AERIAL SURVEYING. BUT, SAYS GUY BUESNEL, THE NAVIGATIONAL CHALLENGES ASSOCIATED WITH UAVS ARE SIGNIFICANT AND THEIR DEPENDENCE ON GNSS FOR PRECISE TIMING AND POSITION MEANS THEY ARE VULNERABLE

UAVs have become an important tool for surveying. Their ability to capture data in locations that would be extremely difficult and time-consuming for someone to access has meant that they have become highly valued for surveying – especially in the energy markets where much of the physical infrastructure (power lines, gas pipelines, oil rigs, chimneys) is very difficult to survey conventionally.

Of course, this means that UAVs have their own set of challenges to face. They must be able to handle a wide range of weather, environmental and radio frequency (RF) signal conditions. They must always know their own position and altitude, and able to navigate a course accurately and return to base safely. They must also stay on the right side of industry regulations, many of which are just starting to be formulated, differ from jurisdiction to jurisdiction, and will almost certainly evolve very fast.

A UAV designer must also consider how GNSS signals will be used. For example, the siting of the GNSS antenna is important, as is the kind and orientation of the antenna during flight operations (pitch, roll, yaw), which will affect the number of satellites in view and the quality of the navigation. Where is the receiver chipset? In the confined space of a UAV, the GNSS receiver is often situated close to other electronics that can interfere with GNSS signals. Are additional sensors required to complement GNSS? Can the positioning system recognise and appropriately correct for errors, such as the aircraft flying upside-down or in an upset state?

As well as dealing with all those aspects, the designer must consider the vulnerability of GNSS to RF interference, atmospheric effects (including scintillation) and even spoofing. This might seem like an unlikely threat but real-world events show that this is no longer the case. In 2012, Todd Humphreys and a team at the University of Texas in the US demonstrated that they could spoof the navigation system of a UAV. In 2015, two Chinese researchers demonstrated how easy it was to build a GPS spoofer using a software defined radio (SDR) that they programmed to be a GPS transmitter. They 'persuaded' a UAV to fly in a geo-fenced restricted area by fooling the navigation system into believing that it was in an unrestricted area in a different country altogether.

The researchers also caused the UAV to crash land in an unrestricted zone by persuading the navigation system the UAV was in a restricted area – the UAV had a safeguard to prevent its engines from working if a user tried to operate it in a restricted zone. This safeguard had obviously not been designed with a spoofing attack in mind and the consequences of a UAV's engines failing as the result of a spoofing attack could be serious.

Also in 2015, the US Department of Homeland Security (DHS) issued a notice stating that criminals had been attempting to jam and spoof their border patrol UAVs. Whilst the DHS did not say whether the attacks had been successful, there was no doubt it regarded the spoofing as a viable threat.

Last year, GPS equipment began malfunctioning just metres from the Kremlin in Moscow. Reports claimed that when close to

Kremlin, GNSS devices reported their position as being close to an international airport miles away from the Kremlin. The zone at and around the international airport was apparently classed as a restricted zone and it was speculated that Russia was implementing an 'anti-UAV' spoofing measure around the Kremlin to prevent UAVs from flying too close.

Now, in 2017, not only do tens of thousands of people understand how to mount a GNSS spoofing attack, the costs of doing so have also fallen considerably – the two Chinese researchers built their spoofer for less than US$1,000. This demonstrates that spoofing is a real threat and even if the spoofer can't control the target GNSS receiver, the fake constellation signals can easily confuse the target systems and cause unexpected effects to occur.

How to beat the spoofer

There are ways to detect that a spoofing attack might be in progress. The spoofer will almost certainly have a higher power level than the signals from the authentic constellation – so a sudden or rapid rise in received signal power can be a good indication of a spoofing attack. Sudden changes to Doppler parameters can also indicate that something untoward is happening. Jumps in position or sudden, unexpected values of data in the navigation messages are all potential indicators of a spoofing attack in progress.

Detection is a good first step – in many applications, it is enough to detect an attack and warn the operator. However, for airborne UAVs, it is obviously insufficient. Control over the UAV needs to be retained, if possible, and any protection mechanism must be carefully designed so that there are no unexpected effects, such as engines shutting down mid-flight.

Possible mitigation for spoofing attacks could include:

- **Multi-frequency receivers:** It is much harder to jam or spoof a GNSS receiver that can receive signals on multiple frequencies.
- **Multi-constellation GNSS receivers:** Receivers that can process signals from multiple satellite constellations (e.g. GPS, GLONASS, BeiDou) are more resistant to all kinds of interference, from obscuration to jamming and spoofing.
- **Improved antennas:** There are many advanced antenna designs available, with a range of form factors and prices, to counteract the effects of jamming and spoofing. The antenna is a vital component of a satellite navigation system and investing a relatively small amount of money here can make a large difference in performance. Advanced military users rely on multi-element antennas that use beamforming techniques to modify the radiation pattern of the antenna to maximise the strength of GNSS signals, while reducing the effect of interference. However, this type of antenna is not available for civilian use.
- **Alternative or backup sources of position, navigation and timing data:** There are many options to explore here, including dead-reckoning sensors, WiFi and cellular-based positioning, assisted GPS, and industry-specific, ground-based back-up/augmentation systems, such as eLoran for maritime use, and WAAS or EGNOS for aviation.
- **Receiver autonomous integrity monitoring:** Techniques in the receiver can detect and exclude signals from their navigation solution if the characteristics are suspicious when compared to other received signals
- **Improved digital signal processing (DSP):** Use DSP technology in the receiver to intelligently monitor signal parameters and excise interfering signals.
- **Use of encrypted GNSS signals:** Encrypted signals are available for use by the US military through the GPS precise positioning service (PPS) and for critical infrastructure in Europe using the Galileo public regulated service.

Detecting a possible spoofing attack and mitigating its consequences have become important for any UAV used in aerial surveying around important infrastructures of the sort found in the energy sector. GNSS receivers in UAVs must be able to detect a spoofing attack. The UAV's navigation system also needs to be able to operate so that the loss of authentic GNSS signals does not compromise the safe operation of the UAV.

This is a unique set of circumstances to meet and requires a degree of robustness higher than that needed for a ground-based system reliant on GNSS. Integration with other sensors on board the UAV such as INS is essential. Fusion with other navigation sensors is also highly desirable, although this is complicated and in its infancy for partly or fully autonomous systems, requiring a combination of artificial intelligence and machine learning algorithms to achieve. Comprehensive tests of the navigation system and mitigation mechanisms against real-world threats is essential and can be simulated to a large degree, meaning that expensive and potentially hazardous test flights can be avoided.

DETECTING A POSSIBLE SPOOFING ATTACK AND MITIGATING ITS CONSEQUENCES HAVE BECOME IMPORTANT FOR ANY UAV

Guy Buesnel is PNT security technologist at Spirent (www.spirent.com)