

SPOOFING: Upping the Anti

GNSS receivers can be fooled, but haven't been much . . . thus far. Should GNSS stakeholders gamble on the status quo? Will widespread spoofing arrive before antispoofing solutions are in place?

Sometimes GNSS spoofing seems a bit like UFOs: much speculation, occasional alarms at suspected instances, but little real-world evidence of its existence.

As far back as 2001, a U.S. Department of Transportation Volpe Center report suggested that as GPS further penetrates into the civil infrastructure, "it becomes a tempting target that could be exploited by individuals, groups or countries".

A recent Department of Home Security (DHS) National Risk Estimate (NRE) of GPS signals that, although jamming disruptions were more likely than spoofing incidents, spoofing is typically of higher consequence than jamming due to the potential duration of time before users or devices would detect spoofing.

Nonetheless, such incidents remain rare.

Iran has claimed to have taken control of U.S. surveillance drones operating along its border. A now well-known demonstration of the same by University of Texas researchers stimulated a Congressional hearing. Last year, Carnegie Mellon University computer science students performed security penetration tests against numerous receiver types and demonstrated not only RF spoofing vulnerabilities but also cyber vulnerabilities and a sensitivity to malformed 50 bps data messages.

So, how great is the risk that spoofing will become a major problem for the GNSS community, and what can we do about it?

To learn more on this subject, we turned to Logan Scott, a consultant specializing in radio frequency (RF) signal processing and waveform design for communications, navigation, radar, and emitter location. Scott has more than 30 years of military and civil GPS systems engineering experience.

What is spoofing?

SCOTT: Spoofing is a process whereby someone (or something) tries to control reported position out of a device. This may take the form of reporting incorrect positioning/velocity/time (PVT) to a local user, or, to a remotely located client. A common misconception is that spoofing is of necessity an RF attack. It is not. In its most general form, spoofing can also involve cyber methods such as malicious software, falsified maps, man-in-the-middle attacks, lying, and so on.

How widespread do you think civil spoofing is?

SCOTT: At present, RF spoofing is mostly a laboratory curiosity, much like computer viruses used to be. Standard signal generators can generate navigationally coordinated signal constellations but absent a knowledge of where the intended victim receiver actually is, they have difficulty generating

a credible set of signals to spoof at a distance. Cyber spoofing is another matter—apps that in effect become a device's location object are readily available for installation on rooted (or jail-broken) smart phones and tablets. Absent secure receiver position signing, intermediate nodes can also falsify reports.

What makes a GNSS receiver vulnerable to spoofing attacks?

SCOTT: First and foremost, a lack of situational awareness. If a receiver looks at received precorrelation power levels using its automatic gain control (AGC), attempts to jam or spoof are usually pretty obvious. Similarly, an examination of post-correlation range/Doppler maps often reveals suspicious responses associated with an RF attack.

Once alerted to the possibility of an attack, receivers can take measures to avoid generating HMI (hazardously misleading information). Finally, we need to recognize that GNSS receivers are connected computers, often running full operating systems. As such, they are subject to a wide spectrum of cyber attacks.

How would you rate the susceptibility of civil receivers to spoofing attacks?

SCOTT: Susceptibility varies widely. A particular problem is that many receivers accept anything that looks like a GPS signal as being authentic



NovAtel's Company Values

Innovation and Integration are cornerstones of our business, we believe that excellence is the standard and we always encourage new ideas.

and they will attempt to synthesize a navigation solution without looking for inconsistencies between signals (detectable via receiver autonomous integrity monitoring, or RAIM) and other navigation sensors. Adding to the problem, GPS is usually by far the most accurate navigation sensor in a suite of sensors and, so, is trusted perhaps more than it should be. For example, exposed to GPS spoofing signals from a signal generator, cellphones will usually opt in to the spoofed GPS solution even though IMU, magnetic, WiFi positioning, and cellular locating solutions clearly show the GPS solution is wrong.

Anti-spoofing solutions tend to fall into receiver-based methods, signal authentication techniques, and GNSS system-based methods. How would you assess the strengths and weaknesses of each category of solutions?

SCOTT: At the receiver, two general types of test, primarily software-based, can be conducted: signals checks and navigation checks. Signals checks focus on looking for RF artifacts such as AGC responses, phase glitches, untoward C/N₀ values, disagreements between L1/L2/L5 measurements, and, unexpected "features" in range/Doppler maps. If multiple antenna inputs are available, a very powerful discriminant is to see if all of the signals come from the same direction. (Hint: they shouldn't).

Navigation checks could include RAIM, looking for disagreements between GNSS systems, unexpected clock states, and – if additional sensors are available – we might look for agreement between GPS results, IMU results, atomic clock time, eLoran, and so forth. These last are potent because they present uncorrelated vulnerabilities – that is, they can't be spoofed by the same measures being directed toward the GNSS receiver.

Although very powerful, the receiver-based solutions are inadequate, particularly when reporting to a remote location. A cyber-attack may use the simple expedient of lying. Cryptographic signal authentication techniques using watermarks can create hard to forge location signatures

useful in proving location to a remote client.

I favor modified civil GPS signal structures designed specifically for this purpose because such an approach serves a wide variety of applications and minimizes trust requirements. Finally, better receiver attestation and map authentication is needed.

What has been the response generally of receiver manufacturers to the threat of spoofing?

SCOTT: In general, manufacturers are becoming more sensitive to the need for high-integrity PVT solutions. They are paying much more attention to receiver heuristics capable of detecting problems and warning users. The upshot is that many receivers are less likely to report severely erroneous positions. The problem for the user community at large is still this: "How do I identify a good receiver?"

Receiver purchasers need mechanisms for selecting receivers that are resistant to RF and cyber attack. To this end, I believe a voluntary, safety-certification program along the lines of Underwriters Laboratory procedures is needed to test receivers for basic compliance. We also need secure mechanisms to establish a receiver's identity and type so that when we plug it into dependent systems, they can be confident of its capabilities.

In general, I oppose any attempts by government to mandate specific requirements except where needed to secure national infrastructure and/or maintain safety of life. That said, the government should take steps to make available needed tools. In particular, civil signals as currently constituted have absolutely no authentication features allowing a user to establish provenance. This is a fundamental mistake in national policy with wide-ranging repercussions. Signal watermarking features are urgently needed to efficiently prove location to remote clients even when under cyber attack. As we build an Internet of things approaching one trillion unique nodes, provable position will gain in importance as an orthogonal layer of defense in depth against cyber attack. 



Logan Scott
LS Consulting

“Many receivers accept anything that looks like a GPS signal as being authentic and they will attempt to synthesize a navigation solution without looking for inconsistencies between signals and other navigation sensors.”



NOVATEL'S SPONSORSHIP Our customers have ideas. Lots of them. Turning those ideas into a competitive advantage is what we do. NovAtel's integrated global positioning solutions deliver success time and time again on land, sea, and in the air. We help many of the world's leading companies stay in the lead by consistently delivering OEM global satellite positioning products that are recognized for their technical innovation, unsurpassed quality and industry-leading customer support.