GPS spoofing

Is your receiver ready for an attack?

Spoofing low-end GNSS devices and mobile phones is relatively easy but how safe is your high-end receiver from an attack?

Will spoofers eat my children?

GNSS users have long been wary about threats from jamming and now a new GNSS bogeyman has appeared. Unlike jamming which is intended to block GNSS signals, spoofers are altogether far more sinister. By replicating GNSS signals, a spoofer can fool a receiver into thinking that it's elsewhere in either time or location. While spoofers may not eat your children, given our reliance on GNSS technology not only for positioning but also timing, it's not hard to imagine the potential havoc that a spoofing attack might cause.

$150 SDRs open spoofing up to the masses

Spoofing has traditionally been an expensive pursuit: tens of thousands of dollars for a GPS simulator–enough to put off most would-be spoofers. In 2013, a well-known demonstration saw a team of researchers from the University of Texas commandeer a 213-foot yacht using $3,000 worth of equipment. More recently, the arrival of cheap Software Defined Radios (SDR), costing as little as $150 combined with the availability of open-source code has made spoofing far more accessible to amateurs on a limited budget.

How will I know if I'm being spoofed?

If you're using a smartphone for positioning, your first inkling of being spoofed would probably be your phone reporting an obviously wrong location. **Figure 2** shows an example of spoofing an iPhone6 into reporting its position at the top of Mount Everest. An Acer Android phone was harder to spoof as additional information from WiFi and the cellular network was also used for positioning. During this test, the phone owner's wife was alerted via Facebook that he had left the country but, spoofing a trip to North Korea might have a slightly less amusing outcome.

In the case of high-end receivers that use multiple frequencies from several satellite constellations, spoofing can be more challenging. If you suspect you're being spoofed, what are the signs to look out for:

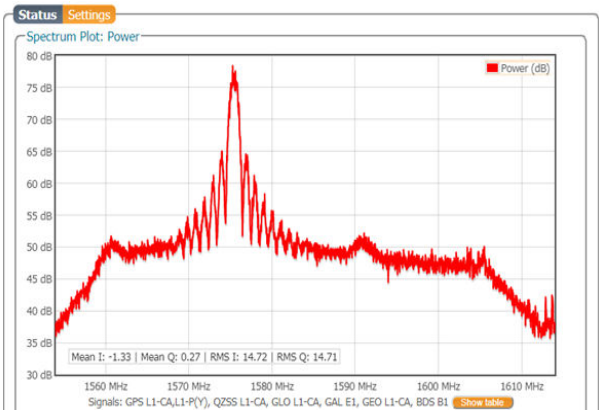

***Figure 1**: The spoofed GPS signal from a HackRF SDR shown in the spectrum plot of the AsteRx-m2a Web Interface. The SDR reproduces the sinc shape of the BPSK signal modulation with a power which in this case, is about 25 dB higher than the real signal.*

The spoofed signal will be visible in the RF spectrum

The low power of GPS signals means that they are barely discernible from the thermal noise background. In order to spoof a receiver, the SDR signals are transmitted with a much higher power making them clearly visible above the background as **Figure 1** shows.

Divergent code - carrier behaviour

Over short time frames, satellite distances measured using the code and carrier phase of the satellite signals should show very little difference - see **Figure 3 (upper panel)**. This behaviour is difficult to replicate so spoofed signals can exhibit a difference that increases rapidly over a short time - **Figure 3 (lower panel)**.

Incomplete and inaccurate nav data

Spoofed satellite navigation data is often missing the GPS constellation almanac and is still only a vague match for the real navigation data.

Jamming of Glonass and/or L2

Spoofing techniques are advancing but at the moment, only the GPS L1 signal is spoofed so a common tactic is to additionally jam the L1 Glonass frequencies and the L2 band. This will manifest as a sudden fallback to a GPS only standalone mode.

What can receivers do about spoofing?

Single-frequency, low-end devices and smartphones are relatively easy to spoof as was shown. High-end multi-frequency receivers have a number of tricks up their sleeve to detect spoofing but what can they do when spoofing has been detected?

Signal integrity alerting

The techniques described above to detect spoofing either directly in the RF spectrum or in the GPS measurements can be employed as spoofing flags.

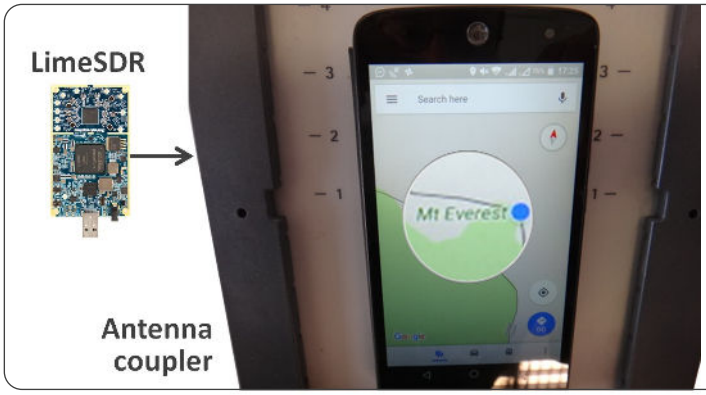

***Figure 2**: Spoofing a smartphone GPS receiver into thinking it's on Mount Everest. A cheap SDR sends a spoofed GPS signal to the smartphone via an antenna coupler.*

Frequency diversity

Having detected spoofing on one frequency, the receiver then switches to using measurements from other frequencies and ignores the spoofed frequency. **Figure 4** shows this technique in action: three receivers are subject to GPS L1 spoofing and, as the spoofer power is increased, the Septentrio AsteRx4 receiver is able to maintain an accurate position by switching from an L1/L2 to an L2/L5 PVT when it detects spoofing on L1.

The other multi-frequency receiver also detects a problem but has no alternative dual-frequency solution so simply stops outputting a PVT. The L1-only module, having no detection mechanisms, switches over to tracking the spoofed signal and it's position gets spoofed.

Inertial sensor integration

An IMU device either coupled to the receiver or mounted on the board itself, provides a unambiguous check for spoofing. In the presence of spoofing, IMUs can also provide input for an integrated PVT solution to mitigate the effects of spoofing.

Staying one step ahead

High-end GNSS receivers, particularly those employing spoofing detection and mitigation methods are still relatively safe from spoofers, however the increasing sophistication of both hardware, in the form of SDRs and open-source software means there's no room for complacency. ■

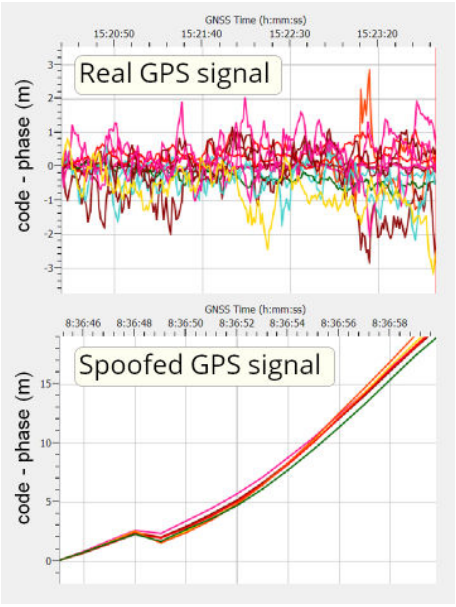

***Figure 3**: Code minus carrier plots for real and spoofed GPS signals. The real signals show a variation around zero whereas the spoofed code and phase diverge rapidly.*

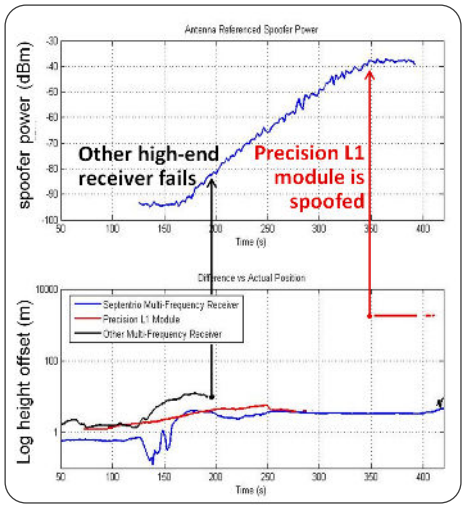

***Figure 4**: Height plot comparison for three different receivers subject to spoofing as the spoofer power is increased. The Septentrio AsteRx4 position survives to maximum spoofer power thanks to frequency diversity.*