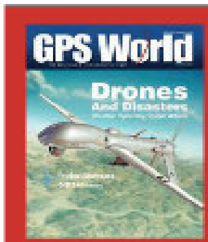
Using One Part of GPS, Ignoring Another

The article "Drone Hack" in the August issue of *GPS World* and Todd Humphreys' testimony before a House Subcommittee overseeing the Department of Homeland Security cited results of a spoofing experiment Humphreys conducted with University of Texas colleagues, demonstrating that a drone helicopter, navigating principally on the civil GPS signal, could have its vertical channel spoofed, causing it to descend. Reaction, quite strong from some directions, prompted one observer to investigate whether a "sky-is-falling" perception is fully warranted. Partly for that reason, emails started circulating among various individuals, including some directly involved in the design. When first brought into the group I was not expecting to be the one to summarize, but, as events unfolded, I'm called on to act as techno-sleuth.

Let me first state the conclusion: the sky is not falling. That's not intended to discourage corrective measures — and it is immediately acknowledged that definitive answers remain unresolved (detailed configuration of the Kalman filter, state estimates, weighting of the baro altimeter). But this much is clear: conditions weren't 100 percent normal. From here I'll cover the supporting facts, followed by possible corrective measures. Discussion will be technical, without any hint of administrative authority or approval.



Conditions were not 100 percent normal in the drone spoofing tests. The sky is not falling.

Key revelations came to light in discussion with the chief scientist of Adaptive Flight, who designed the drone's nav system software and operator interface. "The reason Todd and his team were able to modify the vertical position of the aircraft even though altitude aiding is actually coming from the pressure sensor," he stated, "is that the GPS vertical velocity was being used. The spoofed GPS position (altitude error) was actually being ignored."

We might call that a hybrid mode, using one part of GPS and ignoring another. Selectivity isn't intrinsically unwise — we need options to reject some data without automatically rejecting other information — but, with GPS-derived altitude ignored for any reason, why not reject all vertical-channel influence from GPS? In fact that's consistent with normal operation; disabling (again a quote) "GPS vertical velocity as an aid ... can be done with a command from the control station (and saved as default for the aircraft)."

Well, then, the demo doesn't reflect 100 percent normal procedure. Relief: our drones aren't as vulnerable as we thought, and the fear expressed in various publications can be reduced.

For further support of that conclusion, additional major information from that same designer includes a quote that "The baro altimeter is used to provide a vertical position discrete update to the Kalman filter. This is true for both normal and GPS-denied modes. There are no (automatic) divergence tests in this system. There is some outlier detection/rejection on the GPS (which probably was not triggered in the spoofing tests, but I haven't seen the data). There is nothing on the baro altimeter." Finally, he says "it is a trivial change from the control station to make the vertical channel ignore GPS in normal mode by turning off the down GPS velocity measurement update; it would still fly fine."

The combined weight of all that can justifiably reduce the level of concern — but not all the way down to zero. Now that all this happened, the subject of prevention needs to be addressed.

As Todd Humphreys correctly noted, without spoofing but with existing errors, GPS position updating cannot adequately mitigate low-cost IMU drift. High-end IMUs bring budget issues (and their motion-sensitive errors limit performance anyway). Spectrum and signal quality is seen by many as an important consideration; residual monitoring is another. For the latter to be effective, the existing (loose) coupling needs upgrading (loose coupling wastes information content; the loss is greatest when GPS coverage is marginal). Extent of refinement (tight/ultratight/deep) and usage of carrier phase (while sidestepping its usual traps) open up a subject with much wider scope: cross-checking. I offer just a few fundamentals here.

- Known data-edit capabilities available with existing provisions (for example, baro altimeter cross-checking), rather than something that "can be done" can always automatically disallow any partial influence from GPS instantly upon spoof detection, regardless of its genesis (Kalman filter bias state traceable to past history or any other source).
- the step just noted generalizes to include all sensor data extant onboard, including carrier phase. The specter of huge expense for this particular step is nonessential; some receivers output raw measurements that can be put into public domain algorithms.

See Letters, page 15

Letters

Continued from page 12.

- with access to all the raw data, every solution combination — federated and integrated — can be generated for cross-checking. In all cases, thresholds for residual testing are set with conservative assessments of sensor error statistics; this overbounding enables integrity testing to err on the side of caution (sacrificing some valid data to better ensure rejection of bad). Integrity test algorithms are likewise public domain.

I close by paraphrasing an observation offered by Mitch Narins in a LinkedIn discussion: Deter threats before they happen. With a robust non-GNSS PNT alternative, spoofing will have no affect on safety or security.

— James L. Farrell
President, VIGIL, Inc.
Severna Park, Maryland