
GPS Spoofing in the Middle East Is Now Capturing Avionics



Avionics like those equipping Bombardier's Global 7500 business jet and other commercial aircraft are being "captured" by false GPS broadcasts in the Middle East.

"What we've seen since late September," University of Texas researchers say, "is unprecedented. We have never seen commercial aircraft captured by GPS spoofing before."

Business and commercial aircraft are being led astray thanks to their sensor-fused navigation systems. A series of [spoofing incidents](#) beginning in late September has caused complete aircraft navigational system failures in some airliners and business jets overflying the Iraq- Iran area. As a result, one bizjet almost strayed into Iranian airspace without clearance.

The GPS spoofing has continued and as researchers at the University of Texas at Austin (UT Austin) have sought to pinpoint the sources of the nefarious GPS broadcasts, they have realized that aircraft sent off course by these signals are entirely "captured" by receiving corrupt GPS data which ends up corrupting their backup inertial navigation systems (INS) as well.

"That means that the backup system is no longer reliable as a backup," Todd E. Humphreys, director of UT Austin's radionavigation laboratory.

Humphreys and a graduate student used "observables" obtained from low earth orbit (LEO) satellites to fix the location of a GPS spoofing signal broadcast during the September time period when a series of incidents was first reported.

"The device was on the eastern periphery of Tehran based on many different measurements from many different satellite over-flights," Humphreys explained during a phone interview last week.

He could not reveal which LEO constellation they used to gather the information but it is worth remembering that SpaceX activated links for its Starlink broadband service in Iran following protests there in the aftermath of the death of a young woman arrested by Iranian police for wearing what was deemed to be unsuitable attire in the fall of 2022.

Not long after the series of September spoofing incidents Humphreys' team noted a new source of GPS spoofing in the region emanating from Israel. It picked up a "chirp jammer" broadcasting what Humphreys describes as a sort of "sawtooth" signal. He identified the Israel Defense Forces as the source of the spoofing, likely initiated to keep precision-guided missiles and rockets employed by Hezbollah off balance. The activity was covered in reporting by Israel's *Haaretz* newspaper.

The IDF subsequently acknowledged the jamming and though against international agreements, it has been recognized as a necessary defensive measure. Notably, it has the same effect on aircraft avionics.

This happens when the GPS receivers that are part of aircraft flight management systems (FMS) like Rockwell Collin's [Pro Line Fusion](#) flight deck (which it provides to Bombardier for its Global 7500 and other business jets under the name "Bombardier Vision flight deck") receive spoofed signals.



A Bombardier Global 7500 business jet similar to this one reportedly experienced GPS spoofing over the eastern Mediterranean in late November. The company offered no comment on the issue.

Within the Collins system and similar systems like Garmin's G5000 integrated flight deck, the received GPS data is "fused" - passed directly to the INS portion of the FMS which uses the information to update itself, correcting for the natural drift that inertial reference sensors have and calibrating to the same position that GPS is indicating.

"The GPS receiver eats up that false data and generates erroneous outputs," Humphreys says.

The spoofed signals have thus fooled both the GPS and INS navigation subsystems within the FMS. The resulting inaccurate position information may then be passed on to the aircraft's autopilot, fuel/range calculation and synthetic vision subsystems among others.

Spoofing has effectively captured the airplane and its crew as happened during the incidents reported in September. "This was as dangerous as it gets," Humphreys affirms. "Pilots were as lost as they could get. They had to call air traffic control and ask for turn-by-turn directions.

Humphreys attributes this flaw in modern commercial avionics to the impulse to achieve the best performance in a navigation system working in "normal" (non-disrupted) operating conditions. This approach is seen in the emphasis on connected systems rather than the federated systems of the past.

"You get the connectivity when you let your guard down – when different systems accept the data they get from each other as if it was vetted."

But in the current environment in which aviation and other navigational systems exist, expecting normal conditions to prevail is tantamount to rolling the dice.

"You can't use the fusion techniques that give you the best performance in [present] normal conditions," Humphreys says. "You have to build a level of paranoia into your system that tends to reduce overall performance."

Requiring the GPS and INS portions of integrated avionics systems to check each other, comparing disparities in position information and calculations may seem common-sensical but "it's not integrated in our current avionics," Humphreys acknowledges.

He points out that such cross-checking must be done rigorously, accounting for both spoofed GPS signals and the natural positional drift that comes with INS.

"If the spoofing that's capturing the GPS receiver happens to be spoofing that hasn't pushed you off [course] very far, then there is the possibility that you accept that spoofing even when double checking against the inertial sensor. There are ways a crafty spoofer could capture an aircraft even though the aircraft checks data against its inertial sensor."

Humphreys, who has researched and written about the dangers of GPS spoofing for over a decade and testified before congress on the subject in 2012 and 2015, published a paper in 2016 describing such a sophisticated spoofing exploit which could capture an aircraft's avionics.

But nothing so crafty is as yet being done with GPS spoofing in the Middle East he observes. "What's going on there right now is nowhere near as sophisticated as our attack. It's a blunt instrument and they're falling for it. I think that's a tragedy."

It's a tragedy that continues to be narrowly averted. In late November, flight data intelligence crowdsourcing website [OPSGROUP](#) relayed a report from a flight crew operating a Bombardier Global 7500 business jet in the eastern Mediterranean from Turkey to Cyprus. The route is not far from the Beirut, Lebanon area where, as noted above, Israel has engaged in GPS spoofing.



An image from the flight intelligence website OPSGROUP depicting the GPS spoofing experience by a Bombardier Global 7500 bizjet near Beirut in late November.

OPSGROUP

According to the report, the aircraft was flying at 47,000 feet and the crew had disabled GPS inputs prior to the area based on known spoofing. However, they briefly turned them on again and received spoofed signals. Their FMS showed their (fake) aircraft position as over Beirut, approximately 120 nautical miles away from their real flight path.

I queried both Garmin and Rockwell Collins about the issue of spoofed GPS signals in the Middle East and the susceptibility of their systems to such deception. Garmin's spokesperson emailed a short response saying;

"We are aware of these claims and involved in the appropriate industry committees evaluating detection and mitigation measures for spoofing and jamming, but we'd prefer not to comment further at this time."

A Rockwell Collins spokesman said that the company did not have any comment to make on the issue.

Humphreys pointed out that Europe's Galileo satellite navigation system now includes digital signatures that go with the data it sends to GPS receivers to authenticate their veracity. Similar ideas have been proposed for GPS but as yet not acted on. Even then, they are not foolproof.

Until fixes for the lack of cross checking in navigation systems and GPS itself are made, the danger to commercial and business aircraft from captured avionics as a result of GPS spoofing will remain high.

"I think there are some people who make these avionics systems who are slapping their foreheads right now, saying, 'We probably should have paid more attention to that failure mode and we didn't,'" Humphreys concludes.