

GPS guidance can be fooled, so researchers are scrambling to find backup technologies

March 23 2018, by Samantha Masunaga, Los Angeles Times



Credit: CC0 Public Domain

Five years ago, a team of researchers from the University of Texas at Austin boarded an \$80-million yacht with the intent of trying to fool the vessel's navigation system and stealthily push it off course.

Once the yacht was off the coast of Italy, the team—with the knowledge and permission of the vessel's owner, a wealthy individual who doesn't want to be named—used a briefcase-sized device to slowly drown out legitimate GPS signals and take control of the ship's guidance. It worked. Using the false signals, the team gradually turned the ship while its chart display continued to show it traveling in a straight line.

Since the U.S. developed the Global Positioning System, or GPS, in the 1970s, the nation has become increasingly reliant on this satellite-based method of determining position, time and velocity. Today GPS is used to do everything from calling an Uber and navigating about town to time-stamping financial transactions and dropping guided bombs.

That growing reliance could be a problem, especially if the 30 GPS satellites or their ground stations ever went down, experts say. And that has led a number of government organizations and companies to start thinking about how to fortify the system and whether other signals could be used to supplement or back up the ever-ubiquitous GPS.

In December, Air Force Secretary Heather Wilson told The Times in an interview that "there's not a military mission that doesn't depend on space," and that the Air Force practices as if it didn't have GPS.

Earlier last year, Director of National Intelligence Dan Coats testified before the Senate Select Committee on Intelligence about the future

"global threat of electronic warfare attacks against space systems," such as military satellite communications and GPS satellites. Coats noted that both China and Russia have discussed development of new electronic warfare capabilities.

"For robustness, you really need multiple sources," said Michael O'Connor, chief executive of Satelles, a Herndon, Va., company that has developed a new time and location signal beamed from a separate constellation of satellites that can be used as an alternative or backstop to GPS. "Any one source is vulnerable."

Developed by the U.S. military and offered without charge, the first GPS test satellite launched in 1978. From the beginning, the system was intended for both military and civilian use, with separate signals for each.

GPS was such a "technical marvel" that everyone homed in on using it, said Dave Tremper, program manager in the strategic technology office at the Defense Advanced Research Projects Agency, or DARPA.

GPS satellites send radio signals to receivers on Earth embedded in a car or other object. Using atomic clocks on the satellites, the signal indicates when it was transmitted. The receivers calculate location based on the time the transmission was sent and the time it was received. By combining data from at least four satellites, the receiver can pinpoint where it is.

Over the years, the U.S. military has made improvements and changes to the system.

The civilian signal, which had been intentionally made less precise than the military signal, was expanded and its accuracy improved. New encrypted military signals were added, as was a new frequency largely

for use by the Federal Aviation Administration. Satellites with better technology, precision and resiliency to attacks were launched to replace the old.

These new satellites, known broadly as GPS Block II, have a design lifespan ranging from 7{ years to 12 years. A new generation of satellites known as GPS III, which will have a 15-year lifespan, are under development.

But all of those improvements did not change the fact that there was still just one largely universal system used by the U.S. Other countries and regions have since developed their own versions of GPS, including the European Galileo system and Russia's GLONASS, which can be used free of charge.

Industry experts say GPS is susceptible to a few different forms of attack. One is jamming, in which a GPS receiver is blocked from receiving any information from a satellite. But another, more dangerous concern, is spoofing. As with the UT yacht experiment, a receiver can be fed a false GPS signal, misleading it about its position.

During that experiment, none of the equipment on the yacht's bridge ever set off an alarm, which would have happened if the team tried to jam the GPS signals, said Todd Humphreys, an associate professor in the aerospace department at UT Austin who led the experiment. The team's spoofing was so subtle that the automated systems could not detect that anything was wrong, he said.

Another possibility is a cyber attack against a GPS ground station that could take out the entire system.

"Redundancy has kind of gone away," Tremper said. "We end up now with this single point of failure."

To combat that, government and industry researchers are developing systems and algorithms to collect many different sources of data that could help determine a user's position, assist with navigation or establish the time. Together, those various data sources can be used to double-check the answer given by GPS—or, in the absence of GPS, potentially might be enough to triangulate a location.

One of those data sources could be Satellite Time and Location, also known as STL, a signal delivered by Satellites that can determine position and time independent of GPS.

The service, which began in 2016, was integrated onto a commercial network of satellites operated by Iridium Communications Inc.

Iridium is known for one of the most spectacular bankruptcies ever; it failed in a grand bid to create a mass market for satellite phones, but was reborn as a niche service. Today its so-called constellation of 66 satellites orbits 476 miles above the Earth, closer than the location of the GPS satellites. That proximity yields a stronger signal, according to O'Connor of Satellites.

He said the company works closely with wireless carriers, the U.S. government and a company that fortifies position, navigation and timing sources for businesses.

"GPS is integrated into much more of our lives than people realize," O'Connor said. "It's built into our critical infrastructure."

At DARPA, researchers are working on a project called Adaptable Navigation Systems that would rely on sensors to collect other signals, such as those from mobile networks or commercial satellites. That information would then be translated by the algorithm, fused together, and a location and time would be determined. The 8-year-old program

has been tested in the field on vehicles ranging from Navy destroyers to Army Humvees.

Technology being tested in El Segundo by Aerospace Corp. could eventually pull in even more diverse data sources, such as signals from television antennas, radio stations or even visual imagery, and match those to a location.

A few months ago, a couple of engineers from Aerospace Corp. strapped a specialized antenna on the roof of a car and set off through the streets of El Segundo to see if they could accurately pinpoint their location without using GPS.

As the pair drove around, they checked a laptop in real time to see if their so-called opportunistic navigation sensor was picking up [radio signals](#) that could be used to triangulate their position. Then they compared that dot to the one determined from GPS data.

At one point, the two signals were off by about 65 feet. But at another, the two navigation dots almost exactly overlapped.

The next test of these advanced algorithms, known as Sextant, could incorporate an accelerometer or a visual sensor that could rely on scenery to help navigate, said Randy Villahermosa, executive director of innovation at the nonprofit corporation, which operates a federally funded research and development center focused on space programs for the U.S. Air Force.

Potential applications for a system like Sextant could extend beyond defense to include navigation for autonomous vehicles, he said. Aerospace Corp. does not sell its products commercially.

Industry officials have estimated that the market for GPS products along

with alternatives is already worth a few billion dollars; future uses, such as driverless cars and drones, could dramatically drive up demand.

But it may not be worth it for everyone to switch to a commercial alternative. Just as the original market for Iridium's [satellite](#) phones was undercut by cheap cell service, so businesses may decide to continue taking their chances with GPS.

Each company must determine whether its products require such critical timing that being fooled for even a second would pose a significant risk, said Doug Loverro, former deputy assistant secretary of Defense for space policy and former executive director for the Air Force Space Command's Space and Missile Systems Center.

"I think it depends upon how critical your use is, and whether or not you're in an industry or situation where you have a high risk of being spoofed," he said.

©2018 Los Angeles Times

Distributed by Tribune Content Agency, LLC.

Citation: GPS guidance can be fooled, so researchers are scrambling to find backup technologies (2018, March 23) retrieved 28 April 2024 from <https://techxplore.com/news/2018-03-gps-guidance-scrambling-backup-technologies.html>

<p>This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.</p>
--