GIMME A FIX —

Radio navigation set to make global return as GPS backup, because cyber

GPS killed the radio nav in 2010, but a high-def version is set to return.

SEAN GALLAGHER - 8/7/2017, 8:40 PM

National Air and Space Museum

Enlarge / **This is the way we used to find our way around.**

Way back in the 1980s, when I was a young naval officer, the Global Positioning System was still in its experimental stage. If you were in the middle of the ocean on a cloudy night, there was pretty much only one reliable way to know where you were: Loran-C, the hyperbolic low-frequency radio navigation system. Using a global network of terrestrial radio beacons, Loran-C gave navigators aboard ships and aircraft the ability to get a fix on their location within a few hundred feet by using the difference in the timing of two or more beacon signals.

An evolution of World War II technology (LORAN was an acronym for long-range navigation), Loran-C was considered obsolete by many once GPS was widely available. In 2010, after the US Coast Guard declared that it was no longer required, the US and Canada shut down their Loran-C beacons. Between 2010 and 2015, nearly everyone else shut down their radio beacons, too. The trial of an enhanced Loran service called eLoran that was accurate within 20 meters (65 feet) also wrapped up during this time.

But now there's increasing concern about over-reliance in the navigational realm on GPS. Since GPS signals from satellites are relatively weak, they are prone to interference, accidental or deliberate. And GPS can be jammed or spoofed—portable equipment can easily drown them out or broadcast fake signals that can make GPS receivers give incorrect position data. The same is true of the Russian-built GLONASS system.

Over the past few years, the US Coast Guard has reported multiple episodes of GPS jamming at non-US ports, including an incident reported to the Coast Guard's Navigation Center this June that occurred on the Black Sea. South Korea has claimed on several occasions that North Korea has jammed GPS near the border, interfering with aircraft and fishing fleet navigation. And in the event of a war, it's possible that an adversary could tak [illegible] satellite weapons or some sort of cyber-attack on a satellite network.

As [illegible] e Dan Coates told the Senate Select Committee on Intelligence in May.

> The global threat of electronic warfare (EW) attacks against space systems will expand in the coming years in both number and types of weapons. Development will very likely focus on jamming capabilities against dedicated military satellite communications (SATCOM), Synthetic Aperture Radar (SAR) imaging satellites, and enhanced capabilities against Global Navigation Satellite Systems (GNSS), such as the US Global Positioning System (GPS).

The risk to GPS has caused a number of countries to take a second look at terrestrial radio navigation. Today there's broad support worldwide for a new radio navigation network based on more modern technology—and the system taking the early lead for that role is eLoran. As Reuters reports, South Korea is preparing to bring back radio navigation with eLoran as a backup system for GPS, and the United States is planning to do the same.

Diff-e-q

The eLoran system gets its enhanced accuracy in much the same way that enhanced GPS gear squeezes greater accuracy out of the civil GPS signal for tasks such as surveying and mapping—by using differential correction. A stationary receiver at a known fixed location checks the signal arriving from the beacon and measures the difference between its actual distance from the beacon and the distance calculated from the signal (based on the difference between the signal's timestamp and the time it was actually received).

In differential GPS, the differential information is broadcast by a base station at the known differential point; in eLoran, the data is fed back to the eLoran transmitter, and the transmitter applies the differential correction to its own signal. Since eLoran is regional, the differential calculation remains relatively accurate for its entire coverage area.

Because it uses low-frequency radio waves (in the 90 to 110 kHz range), it's not likely that you'll see eLoran integrated into your smartphone. While the antenna required for receiving eLoran signals is relatively small (about two inches square), that's a fairly massive amount of real estate for a smartphone to dedicate to a backup navigation system. But that size could be reduced with some investment in antenna miniaturization. And while eLoran only works in two dimensions (it doesn't provide altitude data) and only works regionally (with a range of 800 miles), it has one major advantage over GPS: its powerful low-frequency signals are far less susceptible to jamming or spoofing. The signal from eLoran beacons is 1.3 million times stronger than GPS signals. A 2006 MITRE study found that attempts to jam or spoof eLoran would be highly unlikely to work.

"[eLoran] is a deterrent to deliberate jamming or spoofing, since such hostile activities can be rendered ineffective," said Brad Parkinson, the retired US Air Force colonel who managed the original GPS development program, according to Reuters. A report Parkinson contributed to for an Institute for Defense Analyses Independent Assessment Team in 2014 found that "eLoran is the only cost-effective backup for national needs."

The administrations of both George W. Bush and Barack Obama pushed for a national eLoran system, but their efforts were never funded by Congress. However, the version of the Department of Homeland Security funding bill for 2018 just passed by the House of Representatives in July includes language calling for DHS to fund the construction and maintenance of a new eLoran system "as a complement to, and as a backup for" the GPS system. And the South Korean government already has pushed forward plans to have three active eLoran beacons by 2019—that's enough to provide accurate fixes for all shipping in the region should North Korea (or anyone else) attempt to block GPS again.

SEAN GALLAGHER
Sean is Ars Technica's IT and National Security Editor. A former Navy officer, systems administrator, and network systems integrator with 20 years of IT journalism experience, he lives and works in Baltimore, Maryland.

EMAIL sean.gallagher@arstechnica.com // **TWITTER** @thepacketrat

READER COMMENTS 138

SHARE THIS STORY

← PREVIOUS STORY

NEXT STORY →

Related Stories

DARPA program seeks to give subs and undersea drones an acoustic GPS

North Korea pumps up the GPS jamming in week-long attack

GPS jammers and spoofers threaten infrastructure, say researchers

Faster GPS that won't kill your battery via the cloud, and a crowd

Sp

Today on Ars

SUBSCRIPTIONS

Nine Iranians indicted by US for hacking to steal research data

Cambridge Analytica’s London offices raided by British investigators

Tumblr finally names the 84 accounts it says were Russian trolls

A critical analysis of the latest cellphone safety scare

In court, oil companies accept climate science but rewrite its history

Tesla and SpaceX just scrubbed their Facebook pages

Chrome 66 will try to block unwanted noisy autoplaying video

Blind cavefish seem to ignore insulin without health consequences

RSS FEEDS
VIEW MOBILE SITE
ABOUT US
SUBSCRIBE

CONTACT US
STAFF
ADVERTISE WITH US
REPRINTS

NEWSLETTER SIGNUP
Join the Ars Orbital Transmission mailing list to get weekly updates delivered to your inbox.

Email address SUBSCRIBE