How do we keep GPS safe from sabotage?

December 16 2016, by edmund Andrews

Credit: AI-generated image (disclaimer)

Aerial drones are already being used to televise football games, produce 3-D maps and tend farm fields. Uber, the giant ride-sharing company, is now testing a service with self-driving cars in Pittsburgh. China deploys unmanned patrol boats in the South China Sea. Rolls-Royce hopes to launch an unmanned cargo ship by 2020.

But along with all the opportunities, Per Enge, a professor of aeronautics

and astronautics at Stanford, sees a new variation on a familiar threat: cyber hackers. Working alongside Stanford research engineers Todd Walter and Sherman Lo, Enge wants to make sure that the next generation of hackers doesn't wreak havoc by jamming and counterfeiting the navigation signals that keep safety on highways, airways and sea lanes.

"When most people talk about cyber safety, they are usually talking about protecting digital data," says Enge, director of the university's GPS Laboratory. "But talking about cyber safety of a vehicle is brand new, and it's difficult. We've always envisioned a human being at the steering wheel, in the cockpit and in charge of the air traffic control tower."

Threats to autonomous navigation systems come in many forms. Navigation jammers are simple and already commonplace: All they require is a strong radio signal that blocks out the navigation signals from the Global Positioning System and other sources. If there isn't a human in place to re-take control of a car or aircraft, jammers can have lethal consequences.

Enge sees bigger and more complicated dangers lurking in the form of "spoofers," systems that send counterfeit navigation signals to intentionally misdirect a vehicle. Imagine, for example, if a future hacker maliciously scrambled all the location signals in a neighborhood full of autonomous cars.

Enge is on the cutting edge of efforts to spot and foil GPS cyber attacks before self-navigating vehicles become pervasive. Much of his work focuses on ways to toughen up the Global Positioning System, along with Europe's Galileo system, China's BeiDou system and Russia's Glonass system, so that the users can not only identify spoof signals but automatically correct for them.

It is a complex technical challenge for researchers, as well as an issue of contention among policymakers. For one thing, there is a tension between military and civilian interests in the Global Positioning System. It was the U.S. military that originally developed GPS. And while military officials have long supported a publicly available civilian GPS, they worry about exporting cybersecurity technology that might have military value to hostile governments.

Enge and his colleagues believe that many of the solutions lie with innovative new strategies to build on relatively familiar technologies.

In one recent paper, for example, Enge and his co-authors at Stanford and the Federal Aviation Administration described a back-up navigation system for aircraft in case GPS is denied in the continental United States. It would essentially use the existing distance-measuring equipment, or DME, to triangulate a plane's position off the FAA's existing ground-based network of antenna stations.

Another paper describes how to use an airplane's own fuselage as a polarization sieve to identify and then combat both jamming and counterfeit spoof signals. In a recent presentation, Enge and his colleagues showed that measurements from an inexpensive accelerometer were potentially useful for detecting spoofing attacks on a vehicle that is stabilized in one dimension.

Enge and his colleagues are also exploring a way to continuously "truth-check" incoming navigation signals by comparing those that come from U.S. GPS satellites with those sent from European and Russian navigation satellites. The premise is that it is unlikely that all satellites from all systems could be simultaneously spoofed. This last system is called ARAIM, short for Advanced Receiver Autonomous Integrity Monitoring.

To be sure, airplane autopilot and anti-collision systems have had a spectacular safety record for decades.

What's new, says Enge, is a huge looming expansion in both the number and kinds of vehicles that are partly or entirely self-navigating. On top of that, those vehicles are likely to be moving through congested areas. Cars will be navigating along crowded roads and avoiding pedestrians and all manner of unexpected obstacles. Drones could be flying surveillance for office or apartment buildings – or delivering pizza – on every block. For groups bent on inflicting damage and death, the vast increase in such traffic offers an exponential increase in opportunities.

These issues require hard work on many fronts, says Enge – and not just on the technology itself.

"These issues can't be solved with a single stroke of the pen or the keyboard," he says. "It will require legal elements to discourage jamming and spoofing, and social protocols that broadcast the danger of such activities. It will require technical work to toughen the navigation receivers with new satellite signals, digital message authentication, intelligent antennas and much more. Finally, we need to augment current navigation systems with completely independent sources of data on time and location."

Enge is convinced that the challenge is manageable, and that the effort is well worth the benefits that autonomous vehicles offer in safety, efficiency and reduced environmental damage.

"Many have predicted that cyber threats mean that GPS has already reached the peak of its usefulness," he says. "My strong feeling is that GPS is much tougher than critics realize."

More information: Sherman C. Lo et al. Design of a Passive Ranging

System Using Existing Distance Measuring Equipment (DME) Signals & Transmitters, *Navigation* (2015). DOI: 10.1002/navi.83

Single Antenna, Dual Use: Theory and Field Trial Results for Aerial Applications of Anti-Jam and Spoof Detection: waas.stanford.edu/papers/Mcmil … al_print_edition.pdf

Provided by Stanford University