TechXplore

A low-cost, viable solution for self-driving cars to spot hacked GPS

September 7 2022

Credit: Pixabay/CC0 Public Domain

A lot of hurdles remain before the emerging technology of self-driving personal and commercial vehicles is common, but transportation researchers at The University of Alabama developed a promising, inexpensive system to overcome one challenge: GPS hacking that can send a self-driving vehicle to the wrong destination.

Initial research shows a self-driving vehicle can use already installed sensors to detect traveling the wrong route when passengers are unaware of the change, thwarting an attempt to spoof the GPS signal to the vehicle, according to findings outlined in recently published papers in the *IEEE Transactions on Intelligent Transportation Systems* and *Transportation Research Record: Journal of the Transportation Research Board*.

Relying on software code and in-vehicle sensors already part of the self-driving system would be cheaper for consumer and commercial vehicles to deny the hacked directions used to steer cargo or people away from their intended destination, said Dr. Mizanur Rahman, assistant professor of civil, construction and environmental engineering and affiliate researcher with the Alabama Transportation Institute.

"The sensors guiding the vehicles are the same sensors that can be used to detect the fake GPS signal," he said. "If the vehicle has the wrong information and is misguided, this can detect it and get back on track."

While commercially available vehicles have some automation, none have reached the point of full autonomy.

"It may seem futuristic, but we need to think like hackers to address problems before the systems are in place," said Sagar Dasgupta, a doctoral student and corresponding author on those papers. "Self-driving vehicles are coming so we need to make sure users are safe. The vehicles need to be secure, so they are considered safe and reliable."

Automakers are developing cybersecurity software to protect the computers in the vehicles from remote hacking, but GPS signal spoofing is different. A spoofed GPS signal comes from outside the vehicle, leaving the internal computer system alone while it navigates a new route based on faulty information.

"Already a threat to military craft and international cargo shipping, personal vehicles with self-driving features will also need to detect the spoofed signal in real-time to return to the correct route," Rahman said.

Rather than programming the vehicle to computationally analyze and validate the signal, UA researchers created an algorithm that uses built-in in-vehicle sensors that detect acceleration, speed and direction to validate the car's path aligns with the directions desired for the journey.

"Our solution goes to the root of the problem by detecting the location change," Sagar said. "GPS is the most vulnerable component, so we are using the sensors inside the vehicle to detect the GPS spoofing from outside the car."

The researchers used the Honda Research Institute Driving Dataset that contains data of 104 hours of human driving in the San Francisco Bay area in a vehicle equipped with self-driving vehicle sensors. Using the data from those sensors during the drives, the UA researchers simulated how they would respond under a spoof GPS signal.

They developed multiple robust spoofing detection models, finding the models were essentially highly accurate in detecting spoofs.

The next steps for the research will be implemented in vehicles with self-driving features, Sagar said.

"We think this will be one of the security modules in the next generation of self-driving vehicles," he said.

More information: Sagar Dasgupta et al, A Reinforcement Learning Approach for Global Navigation Satellite System Spoofing Attack Detection in Autonomous Vehicles, *Transportation Research Record: Journal of the Transportation Research Board* (2022). DOI: 10.1177/03611981221095509

Sagar Dasgupta et al, A Sensor Fusion-Based GNSS Spoofing Attack Detection Framework for Autonomous Vehicles, *IEEE Transactions on Intelligent Transportation Systems* (2022). DOI: 10.1109/TITS.2022.3197817

Provided by University of Alabama in Tuscaloosa

Citation: A low-cost, viable solution for self-driving cars to spot hacked GPS (2022, September 7) retrieved 5 May 2024 from https://techxplore.com/news/2022-09-low-cost-viable-solution-self-driving-cars.html