New study presents method to stop cyber attacks on GPS-enabled devices

March 19 2018

Credit: CC0 Public Domain

A new study by researchers Nikolaos Gatsis, David Akopian and Ahmad F. Taha and their graduate student Ali Khalajmehrabadi from the UTSA Department of Electrical and Computer Engineering describes a computer algorithm that mitigates the effects of spoofed GPS attacks on electrical grids and other GPS-reliant technologies. This new algorithm has the potential to help cybersecurity professionals to better detect and prevent cyber attacks in real time.

"Malicious agents have the ability to disrupt a device's understanding of time and location by emitting a signal that is pretending to be a GPS signal," Gatsis said. "This can be very harmful in several different realms of technology."

The U.S. electrical power grid, for example, depends on GPS to give time stamps for its measurements at stations across the country. Although reliable, researchers in laboratories across the world have shown that the system can be vulnerable to spoofing cyber-attacks that can disrupt the system's time and location data.

"In broad terms, malicious cyber-attackers can clone the GPS signal and display, for instance, the wrong time or the wrong location," Akopian said. "This can wreak all sorts of havoc. It can send people to the wrong location or render hours of data useless."

The trio's algorithm, which can be applied to cell phones or computers as easily as a new app, has the ability to recognize false GPS signals and counter an attack while it occurs. Their main focus has been preventing attacks on the American electrical power grid, but the algorithm is applicable to several different devices.

"As we move forward with this concept of driverless cars, it becomes much more vital that we secure our GPS signals because the hijacking of the location abilities of a driverless car could be very dangerous," Taha said. "Beyond that, cell phone towers and banks also use GPS signals. Every day, hundreds of thousands of measurements of time and location are made using this information—and it's important to make the data secure."

More information: Ali Khalajmehrabadi et al, Real-Time Rejection and Mitigation of Time Synchronization Attacks on the Global Positioning System, *IEEE Transactions on Industrial Electronics* (2018). DOI: 10.1109/TIE.2017.2787581

Provided by University of Texas at San Antonio