Autonomous vehicles must prepare for jamming and spoofing attacks

Yoshiyasu Takefuji

Jeffrey Mervis wrote an article entitled "Not so fast," published in Science (1). The safety of autonomous vehicles must be largely enhanced because they are connected vehicles. Connections of autonomous vehicles create new security issues. Data from a variety of sensors will be used for controlling an autonomous vehicle. The third party may be able to create forged signals for disturbing and/or hijacking vehicles. Autonomous vehicles must prepare for jamming and spoofing attacks. Autonomous vehicles use GPS sensor, millimeter wave (MMW) radar, LiDAR (light detection and ranging) sensor, ultrasonic sensor, and camera sensor. For example, GPS spoofing became very popular after Pokémon GO hacks. GPS signal spoofing can be easily achieved (2, 3). We must prepare for jamming and spoofing attacks against GPS, MMW, LiDAR, ultrasonic sensor, and camera respectively. Details will be described (4). If we could overcome the problems of jamming and spoofing attacks, dystopian views about autonomous vehicles will be eliminated.

References:

1. Jeffrey Mervis, "Not so fast," Science, 15 Dec 2017, 358 (6369), 1370-1374
2. https://github.com/osqzss/gps-sdr-sim
3. Stefan Kiese, Gotta Catch 'Em All! – WORLDWIDE! (or how to spoof GPS to cheat at Pokémon GO), 2016 https://insinuator.net/2016/07/gotta-catch-em-all-worldwide-or-how-to-spoof-gps-to-cheat-at-pokemon-go/
4. Y. Takefuji, "Connected vehicle security," to appear in IEEE Technology and Society Magazine in 2018.