

Autonomous vehicles must overcome spoofing, silencing, jamming attacks...

Yoshiyasu Takefuji

Lee Vinsel wrote an article entitled “American adventure and autonomous cars” (1). Autonomous vehicles have key sensors including global positioning system (GPS), millimeter wave radar, light detection and ranging (LiDAR), ultrasonic sensor, and camera sensors. They have been weak and vulnerable against spoofing, silencing, and jamming attacks (2). In other words, we must build robust autonomous vehicles against known and unknown adversarial attacks. Otherwise, the autonomous vehicles, and self-driving cars, will become the next crime frontier. In order to build the robust autonomous vehicles, every sensor must be AI-embedded and smart / intelligent enough to overcome the adversarial attacks. AI will play a key role in overcoming autonomous vehicles vulnerabilities.

#### References:

1. Lee Vinsel, American adventure and autonomous cars, Science 12 Jul 2019: Vol. 365, Issue 6449, pp. 130-131
2. Y. Takefuji, "Connected Vehicle Security Vulnerabilities [Commentary]," in IEEE Technology and Society Magazine, vol. 37, no. 1, pp. 15-18, March 2018