The security problems of autonomous vehicles are solvable as long as the facts are disclosed

Yoshiyasu Takefuji

Joan Claybrook et al. wrote an article entitled “Autonomous vehicles: No driver...no regulation?” (1). Scientists and engineers must disclose the facts of problems on the conventional vehicles and the expected autonomous vehicles. I have recently published a paper entitled “connected vehicle security vulnerabilities” where a variety of security problems of the conventional and autonomous vehicles are disclosed (2). In the paper sensor spoofing against GPS, LiDAR (LIght Detection and Ranging), and other sensors can confuse the conventional and autonomous vehicles (2-5). However, the described security vulnerabilities problems against sensors are all solvable as long as the facts are disclosed. Recently, LTE/3G hijacking methods have been disclosed (6). They may cause more severe problems in our society from the viewpoint of security. In order to achieve safe/reliable vehicles, we must regulate the security standard for the conventional and autonomous vehicles. Remember that the conventional vehicles with CAN bus have no security embedded (2-5). If we neglect the facts and the security problems in our vehicles, we will not have the happy future.

References:

1. Joan Claybrook et al., “Autonomous vehicles: No driver...no regulation?” Science 06 Jul 2018: Vol. 361, Issue 6397, pp. 36-37
2. Y. Takefuji, “Connected vehicle security vulnerabilities”, IEEE Technology and Society, pp15-18, March 2018
3. http://science.sciencemag.org/content/352/6293/1573/tab-e-letters
4. http://science.sciencemag.org/content/358/6369/1375/tab-e-letters
5. http://science.sciencemag.org/content/358/6369/1370/tab-e-letters
6. Syed Rafiul Hussain et al., “LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE,” Proc. of Network and Distributed Systems Security (NDSS) Symposium 2018