Cómo proteger los vehículos autónomos de los hackers

Ingeniería, 16/11/2020

Los vehículos autónomos que circulan en la actualidad utilizan sensores, algoritmos complejos y herramientas como GPS, lidar y radar para detectar su entorno y comunicarse entre sí. Los vehículos comparten datos confidenciales para ayudar a disminuir el tráfico y aumentar la seguridad, según un artículo sobre problemas de seguridad en las redes vehiculares de la Biblioteca digital IEEE Xplore. Aunque tener vehículos interconectados puede ayudar a mejorar las condiciones del tráfico, se necesitan medidas de seguridad y privacidad para proteger a los vehículos de los ciberataques.

Los investigadores Charlie Miller y Chris Valasek hackearon éticamente un Jeep Cherokee autónomo de nivel 2 mientras estaba en la carretera. Querían ver cuáles podrían ser las consecuencias. Pudieron detener el vehículo en la carretera, según un artículo de Towards Data Science, y pudieron controlar el volante y la velocidad del vehículo.

Para que los vehículos autónomos se adopten de forma generalizada, debe garantizarse su seguridad. El mantra de un buen ingeniero en el campo es: La ciberseguridad en la tecnología automotriz no es un producto sino un proceso. Es más que diseñar sólidas características de seguridad y protección, para comprender realmente el desarrollo, la recopilación, el análisis, la interpretación de los vehículos inteligentes de los datos de los vehículos conectados y su protección mediante la tecnología blockchain para, en última instancia, asegurar los vehículos autónomos.

Soy Jorge Carlos Fernández Francés, editor, analista y experto en el sector automotriz. Mi experiencia a lo largo de los años, me ha dado la oportunidad de colaborar en distintos medios de comunicación para difundir las últimas noticias sobre el maravilloso mundo del automovilismo.