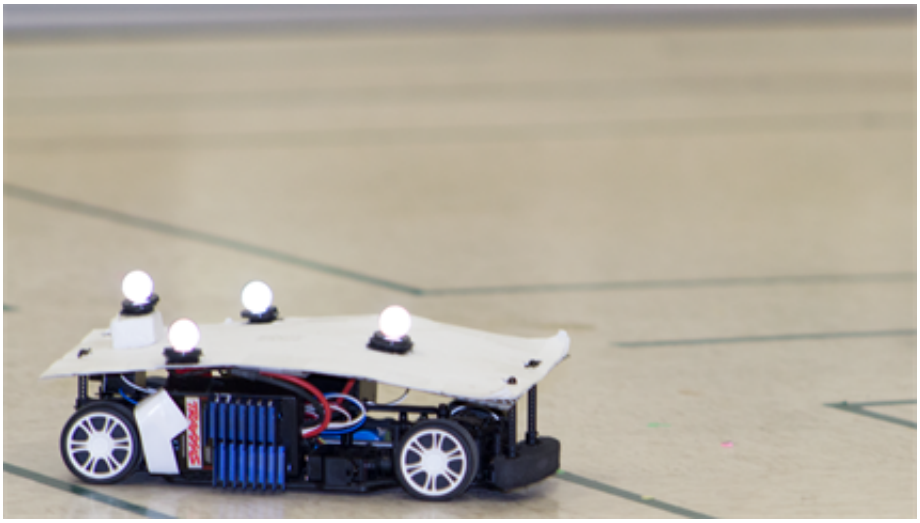
Researchers tackle autonomous vehicle security

May 24 2017



Credit: Texas A&M University

Texas A&M University researchers have developed an intelligent transportation system prototype designed to avoid collisions and prevent hacking of autonomous vehicles. Modern vehicles are increasingly autonomous, relying on sensors to provide information to automatically control them. They are also equipped with internet access for safety or infotainment applications making them vulnerable to cyberattacks. This will only multiply as society transitions to self-driving autonomous vehicles in which hackers could gain control of the sensors, causing confusion, chaos and collisions.

Although autonomous vehicles are essentially large computers on wheels, securing them is not the same as securing a communication network that connects desktop computers and smartphones to large geographical areas due to the roles that the sensors and actuators play in the physical layer of the network.

Working in the Texas A&M's Cyberphysical Systems Laboratory, Dr. P.R.Kumar, University Distinguished Professor in the Department of Electrical and Computer Engineering, along with graduate students Bharadwaj Satchidanandan and Woo-Hyun Ko, have applied the theory of dynamic watermarking of sensors in autonomous vehicles to prevent malicious attacks.

In their research demonstrations, 10 cameras recorded the movement of the self-driving prototype vehicles. The vision sensors in the system received the images and accurately calculated the exact location and orientation of the vehicles. Then they transmitted this information to a server, which in turn controlled the vehicles.

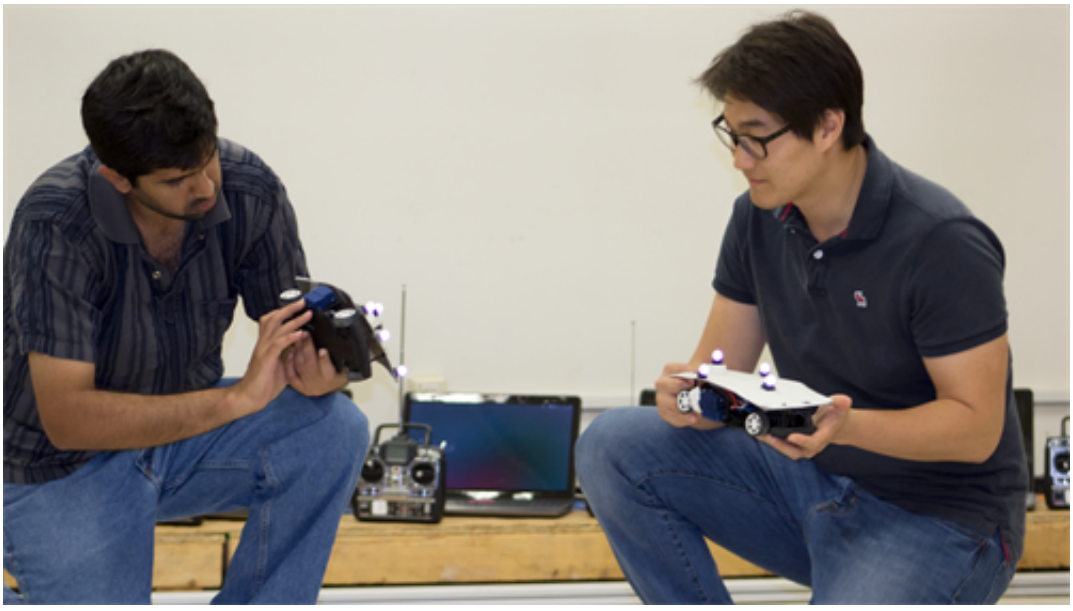
"Sensors are like GPS navigation in the network that gather information about the environment," said Satchidanandan. "Actuators such as motors, or controls such as the steering wheel, interact with them. If the sensors are corrupted or hijacked by malicious agents through the internet, they can provide false information on vehicle locations resulting in collisions."

To fix this, Kumar and his team added a random private signal called a 'watermark' to the actuators. The presence of this watermark and its statistical properties were known to every node in the system, but its actual random values were not revealed. When the measurements reported by the sensors did not have the right properties of this watermark, the actuators assumed that the sensors or their measurements had been tampered with somewhere along the line. With this new

information, the researchers could predict a collision.

The researchers showed that their technology could work in the lab. The actuators in the autonomous vehicles halted themselves when the sensors were tampered with.

"This is an instance of the broader concern of security of cyberphysical systems. The increasing integration of critical physical infrastructures, such as the smart grid or automated transportation, with the cyber system of the internet has led to such vulnerabilities," said Kumar. "If these technologies are to be adopted by society, they will need to be protected against malicious attacks on sensors."



Credit: Texas A&M University

More information: Theory and implementation of dynamic watermarking for cybersecurity of advanced transportation systems.

DOI: 10.1109/CNS.2016.7860529