Knowledge Transfer Office
香港城市大學
City University of Hong Kong

A Method for Protecting Self-driving Cars from Cyber Attacks

- Communications & Information
- Energy & Environment
- Health & Wellness
- Manufacturing

Buildings and Construction Technology
Computer/AI/Data Processing and Information Technology
Consumer Electronics
Electricity and Power Electronics
Robotics
Sensors
Smart Mobility and Electric Vehicle
Testing Instruments

Opportunity

As autonomous vehicle (AV) or connected autonomous vehicle (CAV) being deployed to help minimize roadside deaths/accidents (1.3 million deaths per year worldwide, 37,000 in the US alone in 2106, around 100 billion USD industry- wide has been invested in R&D to provide a solution) due to the human errors, reliability of CAV is of top concern. One of the key challenges and concerns is how to protect a CAV from Cyber attack. Most of the existing solutions use novel intrusion detection schemes or anomaly behavior analysis, yet the mechanism/algorithm itself is within the system of attack possibility, thus creating a single point of failure that will render the entire detection scheme useless.
This invention provides a method to bringing an AV to a safe harbor when it is under a cyber attack

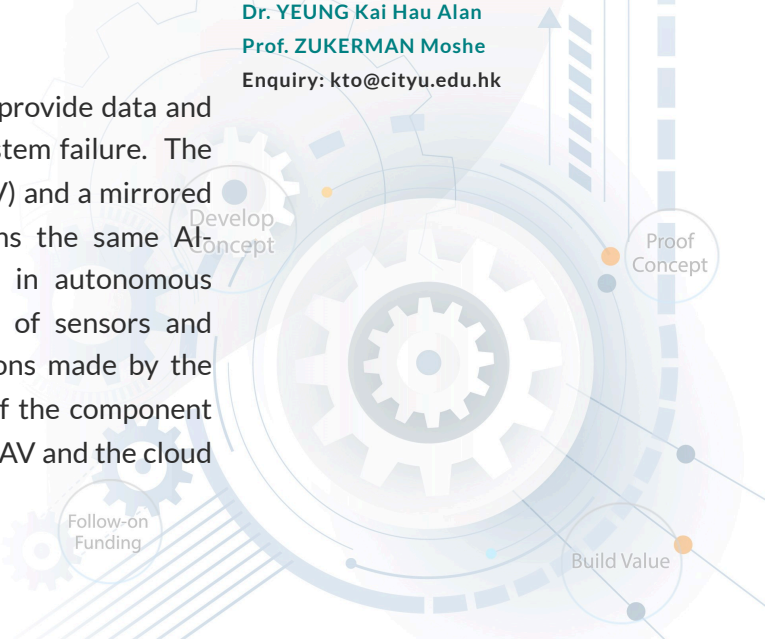
Technology

Mirror technology has been used successfully for years to provide data and system integrity guarantee and fast recovery in case of system failure. The invention proposes to use a duplicate set of sensors (in CAV) and a mirrored processing component in the cloud (this component runs the same AI-enabled real-time controlled optimized motion planning in autonomous mode in the CAV). The purpose of this duplicated set of sensors and processing components is to counter-checking the decisions made by the CAV. Any attack on the CAV will not affect the integrity of the component resident in the cloud, thus any disagreement between the CAV and the cloud

IP Status
Patent granted

Technology Readiness Level (TRL) ? 3

Inventor(s)
Dr. YEUNG Kai Hau Alan
Prof. ZUKERMAN Moshe
Enquiry: kto@cityu.edu.hk



will indicate a potential cyber-attack or local system failure, at that point, the CAV will be forced to stop, and park at the nearest safe harbor point (e.g., parking space).

Advantages

- Compared to the existing fault/cyber- attack detection methods that are prone to the same attack as it is resident in the same area of attack, this invention isolates that possibility by having a mirror detection algorithm in the cloud.

Applications

- Detection of cyber attack on CAV
- Independent detection of mal function in any critical system component