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

一种保护自动驾驶汽车免受网络攻击的方法

- 信息和通信
- 能源和环境
- 健康与保健
- 制造
  - 建筑和施工技术
  - 计算机/人工智能/数据处理和信息技术
  - 消费电子
  - 电力和功率电子
  - 机器人学
  - 传感器
  - 智能出行与电动汽车
  - 测试仪器

机会

由于人为错误造成的道路事故每年导致全球130万人死亡，仅在2016年美国就有37,000人遇难，行业在研发方面投入了约1000亿美元，以提供解决方案。因此，自主车辆（AV）或互联自主车辆（CAV）的部署旨在减少由于人为失误而导致的道路死亡/事故。可靠性是CAV的首要关注点之一。一个主要的挑战和关注点是如何保护CAV免受网络攻击。目前大多数现有的解决方案采用新颖的入侵检测方案或异常行为分析，但这些机制/算法本身依然处于可能被攻击的系统内，从而造成单点故障，使整个检测方案失效。这项发明提供了一种在CAV遭受网络攻击时，将其带入安全港的方法。

技术

镜像技术多年来已成功用于提供数据和系统完整性保证，并在系统故障时实现快速恢复。这项发明提出在CAV中使用一套操作重复的传感器和云端的镜像处理组件（在CAV的自主模式下运行相同的AI驱动实时控制的优化运动规划）。这套重复的传感器和处理组件的目的是对CAV的决策进行核对。对CAV的任何攻击都不会影响云端组件的完整性，因此CAV和云端之间的任何不一致都将表明可能存在网络攻击或本地系统故障，此时，CAV将被迫停止并停泊在最近的安全港点（如停车场）。

优势

- 与现有的易受同样攻击的故障/网络攻击检测方法相比，这项发明通过在云端进行镜像检测算法隔离了这类攻击的可能性。

应用

- CAV的网络攻击检测
- 对任何关键系统组件进行独立检测

IP状态
专利已授权

技术成熟度等级 (TRL) ? 3

发明人
杨启厚
Prof. ZUKERMAN Moshe
询问: kto@cityu.edu.hk