YANG XUEHUAN (SG PR)

Email : s190113@e.ntu.edu.sg

Education

- **Nanyang Technological University(NTU)** — Singapore
  Master of Engineering in Computer Science — *Jan 2020 - Feb 2022*
  - **Thesis**: Simulation-Based perception testing for autonomous vehicles(10356/154942)
  - **Research**: Cyber Security for Autonomous Vehicle
- **Nanyang Technological University(NTU)** — Singapore
  Bachelor of Engineering in Electrical and Electronics — *Aug 2016 - Dec 2019*
  - **FYP**: Interfacing and Testing of Localization Sensors on An Autonomous Vehicle(10356/136704)
  - **Graduate**: With Honours (Distinction)

Papers Accepted

- **ACMMM 2022**: Xingshuo Han, Guowen Xu, Yuan Zhou, **Xuehuan Yang**, Jiwei Li, Tianwei Zhang, Physical Backdoor Attacks to Lane Detection Systems in Autonomous Driving, ACM International Conference on Multimedia (MM), October, 2022

Papers Under Review

- **USENIX 2023**: A Comprehensive Platform for Benchmarking Backdoor Attacks to the Perception Module in Autonomous Vehicles
- **TIFS 2022**: Verifiable, Fair and Privacy-preserving Broadcast Authorization for Flexible Data Sharing in Clouds

Papers Undergoing

- **CVPR 2023**: Dual Key Backddoor Attack for Audio Visual Speech Recognition

Research Experience

- **School of Computer Science and Engineering@NTU** — Singapore
  Research Associate, Cyber Security Team — *July 2022 - Present*
  - **Develop critical ML products, and utilize our 3D maps and real-time sensor data to make better perception results**:
- **Cyber Security Research Centre@NTU** — Singapore
  Research Assistant, Cyber Security Team — *Feb 2020 - June 2022*
  - **Research Topics**: Deep learning systems for self-driving cars are a range of scenarios for self-driving cars. Especially in safety-critical applications.
  - **Research Direction**: It is necessary to build trust and reliability in AI systems in everyday decision-making to build trust and reliability.
- **Centre for Autonomous Robotics Lab, EEE@NTU** — Singapore
  Research Intern, Autonomous Vehicle Localization Team — *Jan 2019 - Dec 2019*
  - **DSTA**: The project focuses on the Safety and Cyber Security of driverless cars, in cooperation with the Singapore Defense Science and Technology Agency (DSTA), ordered by the Singapore Ministry of defense (Future Systems Technology Directorate FSTD)
  - **Autoware**: Collaborated Velodyne LIDAR Delphi RADAR with existing software(ROS) and made essential modifications with autonomous vehicle software
  - **Toyota**: Success applied Object Detection and Object Avoidance for Toyota Coms Car
- **Center for Energy Research Institute@NTU** — Singapore
  Research Intern, Future Mobility Team — *Sep 2017 - Dec 2018*
  - **NTU-JTC-Navya**: Tested NTU-JTC-Navya autonomous shuttle bus on NTU's campus
  - **NTU-Volvo-LTA**: Joined NTU-Volvo-LTA 12-meter autonomous electric bus team

Award

- **Math**: 3rd Place, Chinese Mathematics Olympiad (CMO) Competition hosted by the Chinese National High School Mathematics League
- **Coach**: National Register of Coach and NTU Inline Skating Club Coach