YANG Xuehuan (Singapore Permanent Resident)

Email: s190113@e.ntu.edu.sg

Research Interest

- **Autonomous Drving Security**: My research interests are computer vision, AI security, adversarial attack, object tracking, and other related autonomous driving security tasks.

Education

- **Nanyang Technological University(NTU)** — Singapore
  Master of Engineering in Computer Science(SCSE) — *Jan 2020 - Feb 2022*
  - **Thesis**: Simulation-Based perception testing for autonomous vehicles(10356/154942)
  - **Research**: Attack Autonomous Vehicle LiDAR in simulation environment
- **Nanyang Technological University(NTU)** — Singapore
  Bachelor of Engineering in Electrical and Electronics (EEE) — *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 (arxiv 2203.00858)
- **TIFS 2022**: Verifiable, Fair, and Privacy-preserving Broadcast Authorization for Flexible Data Sharing in Clouds, Transactions on Information Forensics and Security(TIFS)

Papers Under Review

- **USENIX 2023**: A Comprehensive Platform for Benchmarking Backdoor Attacks to the Perception Module in Autonomous Vehicles
- **TIFS 2022**: Identity Based Matchmaking Encryption for Cloud Computing

Papers Undergoing

- **ICCV 2023**: Dual Source Backdoor Attack for Audio Visual Speech Recognition

Research Experience

- **School of Computer Science and Engineering@NTU** — Singapore
  Research Associate, Cyber Security Team — *July 2022 - Dec 2022*
  - **Apollo**: Implement workflows for researchers to evaluate backdoor attack scenarios to attack lane detection in autonomoous driving platform and perform the camera backdoor attack with raining environment in the open source LGSVL simulator.
  - **Point Cloud**: Develop critical machine learning products with real-time lidar sensor data to improve perception performance for LiDAR system. Assess the impact of environmental conditions on Lidar attack, assist develop methods to detect and mitigate data quality impact of adverse environmental factors through experimental design and data mining with research teams.
- **Cyber Security Research Centre@NTU** — Singapore
  Research Assistant, Cyber Security Team — *Feb 2020 - June 2022*
  - **Gap analysis**: Perform the apollo platform for the result of LiDAR perception with the LGSVL ground truth at a low speed for safety-critical applications.
  - **Cyber security assessment**: Develop tools to interactively segment images point clouds to reduce human effort. Train object detection tracking models to pre-label multisensor data from Lidars cameras Explore methods to help customers identify 'interesting' data in huge video datasets, which can be sent for labeling.
- **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). The project studies the cyber security concerns of driverless cars in hardware and software components and systems.

- **Autoware**: Collaborated Velodyne LIDAR & Delphi RADAR with existing ROS software and made essential modifications with autonomous vehicle software
- **Toyota**: Developed Object Detection and Object Avoidance algorithm for Toyota vehicle's safety scenarios using radar sensor.Successfully tested autonomous vehicle localization in CETRAN, Singapore
- **GPS Attack**: Assist the researchers to perform a physical attack on various GPS devices to increase the GPS signal and improve the robustness of the system in this article: Detection and Isolation of Sensor Attacks for Autonomous Vehicles: Framework, Algorithms, and Validation.

- **Centre for Energy Research Institute@NTU** Singapore
  Research Intern, Future Mobility Team *Sep 2017 - Dec 2018*
  - **NTU-JTC-Navya**: Develop safe AV technologies and guarantee the safety of camera functions to verify lane detections using zed cameras on the campus of NTU.
  - **NTU-Volvo-LTA**: Joined 12-meter autonomous electric bus and build up tools to support customers calibrate their sensors with the need for a traditional checkerboard based calibration. Acquired and analyzed 3D stereo camera (ZED) vision data using Nvidia CUDA to detect lane detection task and recognized obstacles using deep learning technologies.

Award

- **Math**: 3rd Place, Chinese Mathematics Olympiad (CMO) competition hosted by the Chinese National High School Mathematics League
- **Chemical**: 3rd Place, Chinese Chemical Olympiad Competition hosted by Anhui Province
- **Merit**: Merit Student in High School by Hefei City
- **Coach**: National International Inline Skating Coach by Inline Certificate Program && Singapore National Register of Coach (NROC) by Sport Singapore && Singapore Ministry of Education (MOE) Instructor && NTU Inline Skating Club Leader and Coach
- **License**: International Driving License class 3 and class 4 for testing autonomous car, bus and sweeper vehicle in Centre of Excellence for Testing & Research of Autonomous Vehicles NTU (CETRAN)