YANG Xuehuan

Email: s190113@e.ntu.edu.sg

Research Interest

- **Autonomous Vehicle Robotics and Physical AI**: My research focuses on advanced computer vision, adversarial machine learning, object detection, and related areas within the realm of autonomous vehicle robotics. Specifically, I aim to explore the integration of physical AI systems to enhance the robustness and efficiency of autonomous vehicles.

Education

- **Nanyang Technological University(NTU)** Singapore
  Master of Engineering in Computer Science(SCSE) *Jan 2020 - Dec 2021*
  - **Thesis**: Simulation-Based perception testing for autonomous vehicles(10356/154942)
  - **Research**: Assisting team with the first physical attack on lane detection systems in autonomous driving, focusing on vulnerabilities and solutions.
- **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 (CCF-A)**: 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 (CCF-A)**: Jianfei Sun, Guowen Xu, Tianwei Zhang, **Xuehuan Yang**, Mamoun Alazab, Robert Deng, Verifiable, Fair and Privacy-preserving Broadcast Authorization for Flexible Data Sharing in Clouds, Accepted by IEEE Transactions on Information Forensics & Security(TIFS)(9969631)
- **TIFS 2022 (CCF-A)**: Jianfei Sun, Guowen Xu, Tianwei Zhang, **Xuehuan Yang**, Mamoun Alazab, Robert Deng, Privacy-Aware and Security-Enhanced Efficient Matchmaking Encryption, Accepted by IEEE Transactions on Information Forensics & Security(TIFS)(10180078)
- **TDSC 2023 (CCF-A)**: Jianfei Sun, Guowen Xu, Hongwei Li, Tianwei Zhang, Cong Wu, **Xuehuan Yang**, Robert Deng, Sanitizable Cross-domain Access Control with Policy-driven Dynamic Authorization, Accepted by IEEE Transactions on Dependable and Secure Computing(TDSC)(10891832)

Research Experience

- **Singpilot** Singapore
  AI Engineer, Physical AI Perception Team *Feb 2022 -*
  - **NTU 1st Toyota COMS AV**: Tested and evaluated localization sensors for autonomous vehicles and documented performance results.
  - **PSA 1st EPM**: Provide the 1st XCMG Electric Prime Mover in PSA, Singapore
  - **PSA 1st HPM**: Provide the 1st XCMG Hydrogen electric prime mover at Singapore Port (Demo)
  - **LTA 1st PPE Detection**: Developed the first AI-based PPE detection algorithm for the LTA Tengah project and demonstrated it at Hong Kong MTR
  - **PSA 3nd APM**: Developed and supported autonomous driving system for Terberg prime movers at PSA Port.
- **School of Computer Science and Engineering@NTU** Singapore
  Research Associate, Cyber Security Team *July 2022 - Dec 2022*
  - **AV 1st Lane Attack**: Conducted experiments and supported the development of a testbed for autonomous vehicle cybersecurity attacks, contributing to the publication of top-tier research paper
  - **Cyber Security**: Assisted the team in publishing research on data cloud encryption for various scenarios in top-tier journals.
- **Cyber Security Research Centre@NTU** Singapore
  Research Assistant, Cyber Security Team *Feb 2020 - June 2022*
  - **AV Testbed**: Tested and prepared data for the autonomous vehicle system on the Apollo platform within the school campus
  - **Model Attack**: Designed models and attack simulations for data sharing scenarios in cybersecurity contexts

- **Centre for Autonomous Robotics Lab, EEE@NTU** Singapore
  Research Intern, Autonomous Vehicle Localization Team *Jan 2019 - Dec 2019*
  - **1st AV Attack in Singapore**: Collaborated with Singapore's Defense Science and Technology Agency (DSTA) on a project commissioned by the Ministry of Defense (Future Systems & Technology Directorate, FSTD), focusing on the safety and cybersecurity of driverless cars. The project addressed cybersecurity risks across hardware, software, and system-level components.
  - **Qualified Testing**: Developed Object Detection and Object Avoidance algorithm for Toyota vehicle's safety scenarios using radar sensor.Successfully tested autonomous vehicle localization in CETRAN, Singapore
  - **1st GPS Attack**: Assisted researchers in conducting physical attacks on GPS devices to test signal amplification and enhance system robustness, as part of the study: Detection and Isolation of Sensor Attacks for Autonomous Vehicles
- **Centre for Energy Research Institute@NTU** Singapore
  Research Intern, Future Mobility Team *Sep 2017 - Dec 2018*
  - **1st driverless shuttle bus** : Developed Safety-First AV technologies and ensured the reliability of camera-based lane detection using ZED cameras on the NTU campus, as part of the NTU-JTC-Navya project
  - **1st autonomous bus in Singapore**: Contributed to Singapore's first 12-meter autonomous electric bus (NTU-Volvo-LTA), developing tools to help customers calibrate sensors without traditional checkerboards. Collected and analyzed 3D stereo camera (ZED) data using NVIDIA CUDA for lane detection and obstacle recognition with deep learning

Award

- **NTU Award**: Graduated With Honours (Distinction)
- **Math Award**: 3rd Place, Chinese Mathematics Olympiad (CMO) competition hosted by the Chinese National High School Mathematics League
- **Chemical Award**: 3rd Place, Chinese Chemical Olympiad Competition hosted by Anhui Province
- **Province Award**: Merit Student in High School by Hefei City

- **Interest**: National Registry of Coaches (NROC) Coach by Sport Singapore && National International Inline Skating Coach Level 1 by Inline Certificate Program && Ministry of Education (MOE) Inline Skating Instructor by MOE Singapore && NTU Inline Skating Club Leader and Coach
- **Driving License**: International Driving License (Class 3, 4, and 5) by Singapore Safety Driving Centre. Operated and tested autonomous Toyota cars, vehicles, sweeper vehicles, and autonomous buses at NTU's Centre of Excellence for Testing & Research of Autonomous Vehicles (CETRAN). Operated electric and hydrogen prime movers at PSA.