YIHAO CAI

Email: yihao.cai@wayne.edu | LinkedIn | Portfolio | GitHub

Mobile: +1 7743123987 | **Address:** 629 W Milwaukee St, Detroit, MI 48202

EDUCATION

Wayne State University **Aug. 2023 – Present**

- **Major**: **Computer Engineering** – **Doctor of Philosophy** (GPA: 3.93/4.0) ***Greater Detroit, MI, USA***
- **Relevant Course**: Robotic Systems, Control Systems, Online Adaptive ML, Directed Research, Doctoral Seminar, etc.

Worcester Polytechnic Institute **Sep. 2021 – May. 2023**

- **Major**: **Robotics Engineering** – **Master of Science** (GPA: 3.8/4.0) ***Worcester, MA, USA***
- **Relevant Course**: Robot Dynamics/Control, Human Robot Interaction, Motion Planning, Operating Systems, etc.

Nanjing University of Posts and Telecommunications **Sep. 2016 – Jun. 2020**

- **Major**: **Telecommunications Engineering** – **Bachelor of Science** (GPA: 3.43/4.0) ***Nanjing, Jiangsu, China***
- **Relevant Course**: Digital Signal Processing, Automation Control Theory, Computer Network, etc.

RESEARCH EXPERIENCE

Wayne State University **Aug. 2023 – Present**

Department of Electrical and Computer Engineering | Graduate Research Assistant ***Detroit, MI, USA***

- Advised by Prof. Yanbing Mao, I conducted self-directed research in Physics-AI, focusing on integrating established physical models with neural networks to enhance system performance. My work specifically addresses safety concerns in autonomous systems, with applications in areas such as unmanned vehicles, self-driving cars, and robotics. I designed and trained physical models in simulation and successfully performed a real-world transfer to a physical quadruped robot.

Technical University of Munich **Apr. 2024 – Jun. 2024**

Cyber-Physical Systems in Production Engineering | Visiting Scholar ***Munich, Bavaria, Germany***

- I collaborate with Prof. Marco Caccamo's group to embed safety layers that accelerate the training and deployment of AI in safety-critical systems. I designed a hybrid architecture incorporating a real-time patch as the high-assurance controller to ensure safety, which I successfully validated on both a virtual cartpole system in simulation and a physical quadruped robot in real world within a Deep Reinforcement Learning framework.

Worcester Polytechnic Institute **Sept. 2021 – Aug. 2022**

Department of Robotics Engineering | Graduate Laboratory Assistant ***Worcester, MA, USA***

- WPI HiRO lab aims at developing effective interfaces to improve teleoperation performance (e.g. increasing awareness, reducing motion sickness) during human robot interaction. One application would be the tele-nursing robots -- I established a VR-based multi-camera platform that facilitates interface design for remote tasks including locomotion and manipulation.

Stanford University **Jan. 2018 – Feb. 2018**

Department of Computer Science | Exchange Student ***Palo Alto, CA, USA***

- As part of an undergraduate academic program, I visited Stanford University as an exchange student -- I took AI-related courses and jointly worked with a group affiliated to the Stanford AI Lab on a computer vision system for intelligent robotic arms.

WORKING EXPERIENCE

ABB Inc. (USA) **Jan. 2023 – May. 2023**

R&D Engineer, Department of Robotics & Discrete Automation | Internship ***San Jose, CA, USA***

- As an R&D engineer, I work on cutting-edge solutions in CV/ML to increase pick-and-place robot performance.
- Build a software framework on Nvidia AI SoC (Jetson Orin) by setting up the GPU computing pipeline (with CUDA, PCL, OpenCV, TensorFlow) and model conversion (TensorRT) for testing and optimizing inference result (5x faster)
- Research & explore the state-of-the-art Transformer-based DLNN model (Mask3D) in 3D semantic instance segmentation to provide alternatives for solving limitations of the current approach by establishing the high-performance training pipeline.
- Innovate a 2D-based approach for 3D point cloud data labeling and batch generation to train customized models.

Hillstone Networks Co., Ltd **May. 2021 – Aug. 2021**

Software Development Engineer, Department of Cloud Security ***Beijing, China***

- Utilize Kubernetes to organize Docker container clusters and design a security scheme following CIS Benchmarks to protect against container threats; Implement RPC frameworks (HTTP, RESTful, gRPC) to build microservice modules using Golang.
- Exposed to Linux kernel and system modules, including SELinux, AppArmor, eBPF and IPC namespace; I create application-level policies for securing interactions among Docker modules (dockerd, containerd and runc, etc.), increasing overall container security performance in business product around 15%

Whale Cloud Technology Co., Ltd **Jul. 2020 – Mar. 2021**

DevOps Engineer, Department of International & Operation Center ***Nanjing, China***

- Configure web environment by building an automation framework using Shell to deploy Java middleware (Nginx/Dubbo/Redis) on server and ensuring security by utilizing Iptables packet filter with other flow analysis tools (Tcpdump/Wireshark).
- Conduct end-to-end product delivery by designing test cases (Functional Test) in agile software development, setting up CI/CD pipeline for blue-green deployment, and maintaining Oracle user databases by creating stored procedure statements.

RESEARCH WORK

Real-Time Patch: Assuring Safety of Learning-enabled Robot Locomotion **Apr. 2024 – Sep. 2024**

- The current reinforcement learning-based control policy is trained in simulation and deployed on a real robot through zero-shot transfer for legged locomotion. However, due to the Sim2Real gap, the pre-trained policy may bring potential safety risks (e.g., robot falls) when executed in the real world. This method is designed to ensure safe robot locomotion in real-world environments. It incorporates a real-time patch, a piecewise linear controller that provides mathematically provable safety guarantees for the robot. The approach utilizes a hybrid architecture that enables the robot to handle uncertainties and safely learn locomotion policies in real-time. All claims in this work have been validated on a Unitree A1 quadruped robot. (***GitHub***) (***Video***)

Simplex-enabled Safe Continual Learning Machine **Feb. 2024 – Jun. 2024**

- The purpose of this design is to enable an agent to safely explore the state space and learn effectively in a real-world environment. The framework features a hybrid architecture with two parallel controllers: a High-Assurance Controller (HAC), designed using Lyapunov Stability Theory (prioritizes safety but has lower performance), and a High-Performance Controller (HPC), implemented as a Deep Reinforcement Learning (DRL) agent with uncertain safety behavior. In real-world control, the framework serves two main functions: 1). Switching to the High-Assurance Controller when the system enters an unsafe but recoverable state, ensuring safety. 2). Using the High-Assurance Controller's actions to correct the unsafe behaviors of the agent. I designed this from scratch and validated its feasibility in simulation with a Cart-Pole system. (***GitHub***) (***Article***)

PROJECT WORK

Hover-Cartpole: A Mobile Platform for Assisting the Blind **Sep. 2023 – Dec. 2023**

- I design and prototype a wheeled robot from hardware to software independently. This physical platform intended to assist the blind individuals with the navigation tasks in daily life. (***GitHub***)
- For software, I integrated a 2D RPLidar with a Raspberry Pi using ROS for autonomous navigation. For hardware, I reverse-engineered a hoverboard motherboard to serve as robot's low-level controller and assembled BLDC motors as power units

Using Reinforcement Learning to Provide More Robust Congestion Control **Sep. 2022 – Dec. 2022**

- To improve congestion control (CC) robustness in TCP layer, I design and implement a distributed RL-based framework in a virtual network environment (Mininet) and extend its interfaces for customized network topology using synthetic data (***GitHub***)
- Make a system analysis and test the final performance by comparing it with other traditional CC algorithms (TCP Cubic) in a three-by-three dumbbell network topology with different metrics (Bandwidth, Router Buffer Usage, etc.)

WPI HiRO (Human-Inspired Robotics Laboratory) Lab Assistant **Aug. 2021 – Sept. 2022**

- I create an IBVS (Image-based Visual Servoing) scheme with two 6-Dof Kinova arms model by combination of Unity3D and ROS for shared autonomous teleoperation which uses Oculus VR headset for remote scenario telepresence (***GitHub***)
- Development of physical wearable system with RealSense Cameras (sensing), HTC VIVE Trackers (body data) and VR Headset (gaze data + presence) in Unity3D using C#. Design user study and analyze data for research on active telepresence (***GitHub***)

National University Sci & Tech Innovation Program – *SLR (Sign Language Recognition)* **Sept. 2018 – Jan. 2020**

- Data Extraction of sign language features from a batch of video frames captured by KinectV2 (using C++) plus image-processing algorithms from OpenCV (Edge Detection, Threshold Segmentation, Image Filtering) for performance optimization. (***GitHub***)
- Implementation of Neural Networks (C3D, LSTM, R(2+1)D, etc.) to train model and model parameters tuning on server

Summer Mathematical Modelling Competition Activity **Jun. 2018 – Sept. 2018**

- Master common mathematical models and algorithms like regression model, correlation analysis and grey prediction, etc.
- Responsible for creating mathematical models applied to daily life and improve the parameters (MATLAB)

University Automation Science Laboratory Robotics Research Project **Jan. 2017 – Dec. 2018**

- Design robot URDF model (using SolidWorks) for simulation and integrate tools/algorithms into the physical robotic platforms (TurtleBot, DOBOT Arm, etc.) to perform some basic tasks (Navigation, Locomotion, Grasping, etc.)
- Build a framework for robot hand-eye coordination system using Halcon and MATLAB, plus implementation of it for object detection and grasping without collision using motion planning algorithms from MoveIt library.

PUBLICATIONS

- **Real-Time Patch: Assuring Safety of Learning-enabled Robot Locomotion** (On Submission)
  Yihao Cai, Hongpeng Cao, Yanbing Mao, Lui Sha, Marco Caccamo **In** *IEEE ICRA 2025*
- **Simplex-enabled Safe Continual Learning Machine** (Under Review)
  Yihao Cai, Hongpeng Cao, Yanbing Mao, Lui Sha, Marco Caccamo **In** *Neural Information Processing Systems (NIPS) 2024*
- **A framework for multimodal sign language recognition under small sample based on key-frame sampling**
  Jianyu Wang, Jianxin Chen, Yihao Cai **In** *Fifth International Workshop on Pattern Recognition (IWPR) 2020*

PEER REVIEW

- *2024 IEEE Transactions on Control of Network Systems (IEEE TCNS)*

HONORS / AWARDS

- Candidate of Tau Beta Pi Honor Society (WPI Massachusetts Alpha Chapter) **2022**
- First Prize in 2018 National Artificial Intelligence Internet Innovation Competition **2018**
- Third Prize in National University Mathematics Modelling Competition **2018**
- Third Prize in 2018 China National Service Robot Competition **2018**
- First Prize in Provincial University Advanced Mathematics Contest **2017**
- Faculty Honors: Faculty Academic Excellence Scholarship, Civilian Award **2016 – 2017**

EXTRA-CURRICULAR ACTIVITIES

- Talent Member of Wayne Robotics Team at Wayne State University **2023 - Present**
- Member of Cyber Security and Rho Beta Epsilon (Robotics) Club in WPI **2021 - 2023**
- Founder Member of University Piobot Robotics Club in NJUPT **2017 - 2019**
  Team Leader of Robotics Arm Team, organizing instruction lessons and participating in national robotics competitions and projects

SKILLS

- **Programming Languages:**
  - C/C++, Python, MATLAB, C#, Shell, Golang, Assembly**,** HTML5/CSS, JavaScript, PL/SQL, VHDL/Verilog
- **AI & Robotics Framework:**
  - ROS, Gazebo/RViz, SLAM, OpenCV/OpenGL, TensorFlow/PyTorch/RLlib, Keras/Caffe, CUDA/cuDNN
- **Tools/Platforms:**
  - **Software:** OmniGraffle, Unity3D, Blender, Wireshark, Mininet, SolidWorks, AutoCAD, IDA Pro
  - **IDE:** Vim/Emacs, Android Studio, VSCode, Eclipse, CLion, PyCharm, Qt Creator, MASM
  - **DevOps/Web:** CMake, Docker/Kubernetes, Oracle Database, Flutter, .Net Framework, Git and SVN