Zhaoyuan Yang

Edison Engineer, Embedded Computing and Machine Learning

EDUCATION

- M.S., Electrical and Computer Engineering, The Ohio State University, 2018
- B.S., Electrical and Computer Engineering, The Ohio State University, 2017

EMPLOYMENT HISTORY

GE Research, Niskayuna, NY

Edison Engineer, September 2018 - Present

- Design cyberattacks detection algorithms for wind power generation systems
- Optimize and deploy deep learning models on different edge platforms
- Analyze different compiler technologies for deep learning models

The Ohio State University, Columbus, OH

Graduate Student Research Assistant, January 2018 - August 2018

- Investigated security applications for connected vehicle technologies
- Designed defense algorithms for adversarial attacks on cyber physical systems

PUBLICATIONS AND PREPRINTS

- Yang, Zhaoyuan, Yang Zhao, Weizhong Yan. "Adversarial Vulnerability in Doppler-based Human Activity Recognition." IJCNN (2020).
- Yang, Zhaoyuan, Nurali Virani, Naresh Iyer. "Countermeasure against backdoor attacks using Epistemic classifiers." SPIE Defense and Commercial Sensing (2020).
- Virani, Nurali, Naresh Iyer, and Zhaoyuan Yang. "Justification-Based Reliability in Machine Learning." *AAAI* (2020).
- Bhushan, Chitresh, Zhaoyuan Yang, Nurali Virani, and Naresh Iyer. "Variational Encoder-based Reliable Classification." ICIP (2020).
- Castro, Margarita, Meinolf Sellmann, Zhaoyuan Yang, Nurali Virani. "Empirical Confidence Models for Supervised Machine Learning." CAI (2020).
- Yang, Zhaoyuan, Naresh Iyer, Johan Reimann, and Nurali Virani. "Design of intentional backdoors in sequential models." *arXiv preprint arXiv:1902.09972* (2019).
- Yang, Zhaoyuan. *Adversarial reinforcement learning for control system design: A deep reinforcement learning approach*. Thesis. The Ohio State University (2018).
- Gupta, Abhishek, and Zhaoyuan Yang. "Adversarial Reinforcement Learning for Observer Design in Autonomous Systems under Cyber Attacks." *arXiv preprint arXiv:1809.06784* (2018).