Yujie Ji

Email : yuj216@lehigh.edu
Mobile : +1-484-541-3708

Education

- **Lehigh University, Algorithmic Learning, Privacy and Security (ALPS)** — Bethlehem, PA
  Ph.D. in Computer Science, Advisor: Prof. Ting Wang, GPA: 3.94/4.0 — *Aug. 2016 – Present*
- **Wuhan University, Big Data and Cloud Computation Laboratory** — Hubei, China
  Bachelor of Engineering in Software Engineering, GPA: 3.5/4.0 — *Sept. 2012 – Jun. 2016*

Research Experiences

- **Attack and Defense against Pre-trained Learning System** — Feb. 2017 - Present
  Research Assistant — *Lehigh University, PA, USA*
  - Revealed security risks of reusing pre-trained models in building Machine Learning systems;
  - Designed and implemented attack mechanisms to trigger the misclassification of the transfered model.
- **Detection of Adversarial Samples on Deep Neural Network** — Oct. 2016 - May. 2018
  Research Assistant — *Lehigh University, PA, USA*
  - Analyzed adversarial samples inference behaviors on variety models utilizing Information Theory;
  - Proposed and implemented an adversarial sample detection mechanism to improve model's robustness;
  - Implemented a DNN model compression method based on Network Trimming.
- **Three-dimensional Subway Fire Evacuation Simulation Model** — May. 2015 - Sep. 2015
  Undergraduate Research Assistant — *Wuhan University, Hubei, China*
  - Simulated evacuation strategies inside subway stations based on optimized A* routing algorithm.
- **Chinese Social Media Analysis for Disease Surveillance** — Oct. 2014 - Dec. 2014
  Undergraduate Research Assistant — *Wuhan University, Hubei, China*
  - Predicted the outbreak of flu based on traditional Machine Learning classification algorithms.

Work Experiences

- **Long Sentence Prediction** — May. 2018 - Aug. 2018
  Algorithm Engineer(intern) — *Kika Tech, Inc., Beijing, China*
  - Implemented long sentences prediction based on Seq2Seq model;
  - Cleaned the corpus based on parsing tree analysis.

Publication

- **Yujie Ji**, Xinyang Zhang, Shouling Ji, Xiapu Luo, Ting Wang. Model-Reuse Attacks on Deep Learning Systems. *The 25th ACM Conference on Computer and Communications Security (CCS '18').*
- **Yujie Ji**, Ting Wang. Towards Understanding the Dynamics of Adversarial Attacks [poster]. *The 25th ACM Conference on Computer and Communications Security (CCS '18).*
- Xinyang Zhang, **Yujie Ji**, Chanh Nguyen, Ting Wang. DeepClean: Data Cleaning via Question Asking. *The 5th IEEE International Conference on Data Science and Advanced Analytics (DSAA '18).*
- **Yujie Ji**, Xinyang Zhang, Ting Wang. Backdoor Attacks against Learning Systems. *IEEE Conference on Communications and Network Security (CNS) 2017.* **Best Paper Award.**
- Xiaohui Cui, Nanhai Yang, Zhibo Wang, Cheng Hu, Weiping Zhu, Hanjie Li, **Yujie Ji**, Cheng Liu. Chinese social media analysis for disease surveillance. *Pers Ubiquit Comput (2015) 19:11251132.* (SCI, IF: 1.518).

Skills & Techniques

Languages: Python, Java; MySQL; MATLAB.
Technologies: Linux; PyTorch, Keras, TensorFlow, Theano, Lasagne.