Wenqi Wei

https://wenqiwei789.github.io/Homepage/

Email : wenqiwei@gatech.edu
Mobile : +1-404-213-8068

Education

- **Georgia Institute of Technology** Atlanta, GA
  Ph.D. student in Computer Science *Aug. 2017 to present*
  Areas of interest: big data analytics, machine learning (current focus on deep learning, adversarial learning), privacy-preserving machine learning, data privacy.
- **Huazhong University of Science and Technology** Wuhan, China
  Bachelor of Engineering in Electronics and Information Engineering *Sept. 2013 to June. 2017*
  Graduated with Honors

Research Experience

- **Georgia Institute of Technology** Atlanta, GA
  Distributed Data Intensive Systems Lab *advisor: Prof. Ling Liu*
  Graduate Research Assistant(Aug 2017 - present)
  - **Adversarial Deep Learning: Attacks and Defenses**: Research on how the adversarial model are generated and how to defend the attack caused by the perturbed data.
  - **Privacy Preserving Deep Learning**: Research on providing privacy preserving deep learning models. The idea is to design deep learning models that could provide accurate results while preserving data privacy. All the (hyper)parameter tuning, neural network model design are under Tensorflow. The main techniques for privacy preservation come from differential privacy.
  - **DeepEyes: Deep Learning Powered Localization System with Multi-modal Sensors**: Research on deep learning powered real-time localization system.
- **Huazhong University of Science and Technology** Wuhan, China
  Signal Processing and Information Networking in Communication Lab *advisor: Prof. Pan Zhou*
  Undergraduate Research Assistant(Sept 2015 - June 2017)
  - **Bandit based Online Learning**: Research on designing contextual multi-armed bandit-based recommendation for social network advertising big data. Besides, I worked on designing a contextual X-armed bandit-based recommendation for self-diagnosis in ubiquitous healthcare(Undergraduate thesis).
  - **Learning with Differential Privacy**: Research on designing differentially private online learning algorithm for social network advertising big data to protect user's personal information while providing them with nearly accurate advertising recommendation. Besides, I worked on differentially private mechanism design in large-scale spectrum sharing, hoping to protect the privacy of the user's personal information in spectrum sharing setting.
  - **Algorithmic Game Theory**: Research on algorithmic game-theoretical mechanism design for improving utility of large-scale spectrum sharing. We took truthfulness into account to ensure that users are reporting their actual spectrum demand to our aggregative game model. So that a approximate Nash Equilibrium can be reached.

Publications

[1] Pan Zhou, Wenqi Wei(co-first author), Kaigui Bian, Dapeng Oliver Wu, Yuchong Hu, Qian Wang. "Private and Truthful Aggregative Game for Large-Scale Spectrum Sharing", IEEE Journal on Selected Areas in Communications, 35(2), 463-477,2017.
[2] Wenqi Wei, Ling Liu, Yanzhao Wu. "Characterization of Adversarial Attacks in Deep Learning" (In progress)
[3] Yanzhao Wu, Ling Liu, and Wenqi Wei, "A Performance Comparison of Deep Learning Frameworks" (In progress)
[4] Ling Liu Wenqi Wei, and Yanzhao Wu, "DeepEyes: A Deep Learning Powered Multi-modal Localization System" (In progress)

Skills

- **Language**: Python, Tensorflow, C, HTML, SQL, Verilog HDL, assembly.
- **Tools**: matlab, Latex, Git, CCS(TI DSP), Quartus, Xilinx ISE, FPGA, SPSS.