Wenqi Wei

wenqiwei@gatech.edu —wenqiwei789.github.io/Homepage/

Education

- **Georgia Institute of Technology** — Atlanta, GA
  Ph.D. student in Computer Science — *Aug. 2017 to present*
  Areas of interest: data-driven topics including big data systems, machine learning systems (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)
  - **Machine Learning**: Research on deep learning algorithm and online learning algorithm based system, including algorithm and system design, performance measurement and parameter tuning.Now working on DeepID-based robust multiple class verification system.
  - **Privacy and System**: Research on providing privacy preserving machine learning models that could give accurate results while preserving data privacy, usually in terms of differential privacy.
  - **Adversarial Deep Learning: Attacks and Defenses**: Research on generating adversarial examples and defending against adversarial samples.
  - **DeepEyes: Deep Learning with Crowdsourcing for real-time Localization**: Research and development of infrastructure-free localization system and service with DeepID-based multi-class identification and crowdsourcing.
  - **DLBenchmarking**: Research on characterizing different deep leaning framework benchmarks.
- **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, and 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, which protect the privacy of the user's personal usage information in large-scale spectrum sharing.
  - **Algorithmic Game Theory**: Research on algorithmic game-theoretical mechanism design for improving utility of large-scale spectrum sharing. Truthfulness is into account to ensure users are reporting their actual spectrum demand to our aggregative game model. So that an 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] Ling Liu, Yanzhao Wu, Wenqi Wei, Wenqi Cao, Semih Sahin, Qi Zhang. "Benchmarking Deep Learning Frameworks: Design Considerations, Metrics and Beyond", 38th IEEE International Conference on Distributed Computing Systems, 2018. (submitted)
[3] Wenqi Wei, Ling Liu, Stacey Truex, Lei Yu, Emre Gursoy, Yanzhao Wu"Demystifying Adversarial Behaviors in Deep Learning" (In progress)
[4] Wenqi Wei, Yanzhao Wu, Ling Liu,"DeepEyes: Integrating Deep Learning and Crowd Sourcing for Localization", Southern Data Science Conference, Atlanta2018 (research track poster)
[5] Yanzhao Wu, Ling Liu, Calton Pu, Wenqi Wei, "GIT_DLBench: A Benchmark Suite for Deep Learning Frameworks: Characterizing Performance, Accuracy and Adversarial Robustness" (In progress)

Skills

Python, Tensorflow,matlab, Latex, C, HTML, SQL, Javascript, Git, SPSS Verilog HDL, assembly.