Zonghao Huang

Master student from School of Electrical and Computer Engineering, Oklahoma State University, Stillwater, USA.
Email: zonghao.huang@okstate.edu | Homepage: https://zonghaohuang007.github.io/home/
Address: General Academic Building B07, Oklahoma State University, Stillwater 74075, OK

Research Interest

My current research focuses on information privacy and security in data analytics techniques including machine learning and geo-statistics. I am especially interested in the theoretical aspects on applying differential privacy in machine learning.

Education

Oklahoma State University, Stillwater, USA
Master of Science in Electrical Engineering (by thesis); GPA: 3.76/4.0 *January 2017 - December 2019 (Expected)*
Thesis: *Differentiallly Private ADMM for Privacy-Preserving Distributed Learning*

Nanyang Technological University, Singapore
Master of Science in Electronics (by coursework) *July 2015 - June 2016*

Xiamen University, China
Bachelor of Engineering in Electronics & Information Engineering: GPA: 3.51/4.0 (top 10%) *September 2011 - July 2015*

Work Experience

Graduate Teaching Assistant
School of Electrical and Computer Engineering, Oklahoma State University, Stillwater, USA *August 2019 - present*
Course: *ECEN 4024 Senior Design 2*

Graduate Research Assistant
School of Electrical and Computer Engineering, Oklahoma State University, Stillwater, USA *January 2017 - July 2019*

Refereed Publications

- **Zonghao Huang**, Miao Pan, Yanmin Gong, "Robust Truth Discovery Against Data Poisoning in Mobile Crowdsensing", *IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA, 9-13 December, 2019.*
- **Zonghao Huang**, Rui Hu, Yuanxiong Guo, Eric Chan-Tin, Yanmin Gong, "DP-ADMM: ADMM-based Distributed Learning with Differential Privacy", *accepted for publication in IEEE Transactions on Information Forensics and Security (TIFS), August, 2019.*
- **Zonghao Huang**, Yanmin Gong, "Differential Location Privacy for Crowdsourced Spectrum Sensing", *IEEE Conference on Communications and Network Security (CNS), Las Vegas, USA, October 9-11 (pp. 1-9), 2017. (acceptance rate: 29.9%)*

Research Projects

- **Task Allocation in Crowdsourced Spectrum Sensing with Location Privacy Protection**
  - Identify the challenges of using crowdsourced mobile users for spectrum sensing and propose an approach for allocating tasks to mobile users without access to their individual locations.
  - Propose to use private spatial decomposition to represent mobile users' location data and design an approach to add differentially private noise that provides a good trade-off between privacy and utility.
  - Use MATLAB to conduct simulation on real-world datasets to show the effectiveness of the proposed approach.
- **Distributed Machine Learning with Data Privacy Guarantee**
  - Design a novel differentially private ADMM-based distributed learning algorithm called DP-ADMM, which combines an approximate augmented Lagrangian function with time-varying Gaussian noise addition in the iterative process to achieve higher utility for more general objective functions than prior works under the same differential privacy guarantee.
  - Use the moments accountant method to analyze the total privacy loss and provide a tight end-to-end differential privacy guarantee for DP-ADMM.
  - Provide rigorous convergence and utility analysis of the proposed DP-ADMM.
  - Conduct extensive simulations by MATLAB based on real-world datasets to validate the effectiveness of DP-ADMM in distributed learning settings.
- **Discovering Truth from Conflicting Sensory Data in Mobile Sensing in the Presence of Data Poisoning**
  - Design an optimal data poisoning attack strategy in truth discovery system, which is formulated as a bi-level optimization problem.
  - Propose a robust truth discovery algorithm, which integrates source evaluation and source filtering process into the truth discovery method. The source evaluation estimates the error bias and variance of the sources, and the source filtering process uses the estimated bias and variance as the criteria to remove unreliable sources.

- Conduct experiments by MATLAB on real-world data to show that our approach could provide accurate and reliable results in the presence of data poisoning attacks.

- **Radio Environment Map Construction with Location Privacy Protection**
  - Investigate location privacy in crowdsourced-based radio environment map construction and adopt perturbation mechanism in Ordinary Kriging to provide differential privacy.
  - Use MATLAB to simulate our approach on real-world data to show the privacy-utility trade-off.

Awards and Honors

- **Graduate Teaching Assistantship**, School of Electrical and Computer Engineering, Oklahoma State University, Stillwater, USA, 2019
- **Student Travel Grant for IEEE CNS 2017**, National Science Foundation and Army Research Office, USA, 2017
- **Graduate Research Assistantship**, School of Electrical and Computer Engineering, Oklahoma State University, Stillwater, USA, 2017, 2018, 2019
- **First-Class Scholarship of Academic Excellence**, Department of Electronic Engineering, Xiamen University, China, 2015, 2013, 2012
- **Scholarship of Recreation and Sports**, Department of Electronic Engineering, Xiamen University, China, 2015
- **Second-Class Scholarship of Academic Excellence**, Department of Electronic Engineering, Xiamen University, China, 2014
- **Merit Student Award**, Department of Electronic Engineering, Xiamen University, China, 2012

Academic Activities

- **Reviewer for Conference Manuscript Submissions** :
  - IEEE INFOCOM 2018, IEEE ICC 2018, IEEE CNS 2018.
- **IEEE Student Member**: Communication Society

University Activities

Oklahoma State University International Student Organization International Olympics 2019
Badminton men single bronze medal winner. *September 2019*

Oklahoma State University International Student Organization International Olympics 2018
Badminton men single silver medal winner. *September 2018*

Oklahoma State University National Lab Day
Our lab hosted Guthrie High School students and demonstrated our research projects to the students. *May 2018*

Technical Skills and Languages

- **Programming Languages**: MATLAB, C, Python, Latex, Verilog
- **Languages**: English (proficient), Chinese (native), Cantonese (native)

References

Dr. Subhash Kak: subhash.kak@okstate.edu
Regents Professor, School of Electrical and Computer Engineering, Oklahoma State University, Stillwater, OK, USA

Dr. Jerzy Krasinski: krasins@okstate.edu
Professor, School of Electrical and Computer Engineering, Oklahoma State University, Stillwater, OK, USA

Dr. Ye Liang: ye.liang@okstate.edu
Associate Professor, Department of Statistics, Oklahoma State University, Stillwater, OK, USA

Dr. Chaoyue Zhao: cyzhao@uw.edu
Assistant Professor, Industrial & Systems Engineering, University of Washington, Seatle, WA, USA