

Zonghao Huang

Email: zonghao.huang@okstate.edu | Homepage: <https://zonghaohuang007.github.io/home/>

Mobile: +86 13702956940 | Skype: live: huang_zonghao

RESEARCH INTEREST

- Trustworthy Machine Learning, Differential Privacy, Stochastic Optimization, Data Privacy and Security, Learning Theory

EDUCATION

Oklahoma State University, Stillwater, USA

Master of Science in Electrical Engineering (by thesis); GPA: 3.79/4.0

Jan. 2017 - Dec. 2019

Thesis: Differentially Private ADMM for Privacy-Preserving Distributed Learning

Nanyang Technological University, Singapore

Master of Science in Electronics (by coursework)

Jul. 2015 - Jun. 2016

Xiamen University, China

Bachelor of Engineering in Electronic & Information Engineering; GPA: 3.51/4.0 (rank: 10/106)

Sept. 2011 - Jul. 2015

Honor: Graduated with First-Class Scholarship of Academic Excellence (top 10%)

WORK EXPERIENCE

Graduate Teaching Assistant

School of Electrical and Computer Engineering, Oklahoma State University, Stillwater, USA

Aug. 2019 - Dec. 2019

Course: ECEN 4024 Senior Design 2

- Organized students' exams and managed Senior Design 2 Lab.

Graduate Research Assistant

Network Information Security and Privacy Lab, Oklahoma State University, Stillwater, USA

Jul. 2018 - Jul. 2019

- Researched on privacy-preserving distributed machine learning.
- Researched on robust truth discovery against data poisoning.

Graduate Research Assistant

Advanced Technology Research Center, Oklahoma State University, Stillwater, USA

Jan. 2017 - Jun. 2018

- Researched on privacy-preserving distributed machine learning.
- Researched on crowdsourced spectrum sensing with location privacy guarantee.

PUBLICATIONS

• Peer-Reviewed Journal Papers:

- Zonghao Huang, Rui Hu, Yuanxiong Guo, Eric Chan-Tin, Yanmin Gong, “[DP-ADMM: ADMM-based Distributed Learning with Differential Privacy](#)”, *IEEE Transactions on Information Forensics and Security (TIFS)*, vol. 15, pp. 1002-1012, 2020. (impact factor: 6.211)

• Peer-Reviewed Conference Papers:

- 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, 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%)

• Papers under Submission:

- Zonghao Huang, Yanmin Gong, “[Differentially Private ADMM for Convex Distributed Learning: Improve Accuracy with Multi-Step Approximation](#)”, under submission.

RESEARCH PROJECTS

• Privacy-Preserving Distributed Machine Learning

Jul. 2017 - Dec. 2019

- Proposed a novel differentially private ADMM-based distributed learning algorithm called DP-ADMM.
- Adopted an approximate augmented Lagrangian function with time-varying Gaussian noise addition in the ADMM iterative process to achieve higher utility for more general objective functions than prior works under the same differential privacy guarantee.

- Used the moments accountant method to analyze the total privacy loss and provide a tight end-to-end differential privacy guarantee for our approach.
 - Completed the 1st work to provide theoretically rigorous convergence and utility analysis for differentially private ADMM.
 - Conducted simulations by MATLAB based on Adult Dataset to demonstrate that our approach achieves better accuracy compared with prior works (improving accuracy by 4.5% and 2.75% when ϵ is 0.05 and 0.1 respectively).
 - Published one paper in IEEE Transactions on Information Forensics and Security, a top journal on information security.
 - Extended and improved DP-ADMM by allowing l approximate primal variable updates in each ADMM iteration.
 - Provided both theoretical analysis and numerical results to demonstrate the accuracy improvement.
- **Discovering Truth from Conflicting Sensory Data in Mobile Sensing in the Presence of Data Poisoning** *Jul. 2018 - May 2019*
- Designed an optimal data poisoning attack strategy in truth discovery system and formulated it as a bi-level optimization problem.
 - Proposed a robust truth discovery algorithm by integrating additional source evaluation and source filtering process into the truth discovery method.
 - Formulated source evaluations as optimization problems to estimate the error bias and variance of the sources, and used a threshold-based source filtering method to remove unreliable sources according to the estimated bias and variance.
 - Conducted 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 (reducing accuracy loss by 33.9% when the attacker ratio is 20%).
 - Published one paper in IEEE Global Communications Conference 2019.
- **Location Privacy-Preserving Crowdsourced Spectrum Sensing** *Jan. 2017 - Dec. 2018*
- Identified the challenges of using crowdsourced mobile users for spectrum sensing and proposed an approach for allocating tasks to mobile users without access to their individual locations.
 - Proposed to use private spatial decomposition to represent mobile users' location data and designed a differentially private spatial decomposition based on truncated geometric mechanism that provided a good trade-off between privacy and utility.
 - Used MATLAB to conduct simulation on real-world datasets to show the effectiveness of the proposed approach.
 - Published one paper in IEEE Conference on Communications and Network Security 2017.
 - Adopted Ordinary-Kriging to construct radio environment map for dynamic spectrum access management.
 - Adjusted Ordinary-Kriging by considering the variance of introduced noise to improve the utility while providing geo-indistinguishability (location privacy guarantee).

AWARDS AND HONORS

- **Student Travel Grant for IEEE CNS 2017**, National Science Foundation and Army Research Office, USA, 2017
- **First-Class Graduate Scholarship of Academic Excellence**, Xiamen University, China, 2015
- **Graduate Scholarship of Recreation and Sports Excellence**, Xiamen University, China, 2015
- **Second-Class Scholarship of Academic Excellence**, Xiamen University, China, 2014
- **First-Class Scholarship of Academic Excellence**, Xiamen University, China, 2013, 2012
- **Merit Student Award**, Xiamen University, China, 2012

ACADEMIC ACTIVITIES

- **Reviewer for Conference Manuscript Submissions :**
 - IEEE International Conference on Computer Communications (INFOCOM) 2018;
 - IEEE International Conference on Communications (ICC) 2018;
 - IEEE Conference on Communications and Network Security (CNS) 2018.
- **IEEE Student Member:** Communication Society
- **Conference Presentation:**
 - "Differential Location Privacy for Crowdsourced Spectrum Sensing", *IEEE Conference on Communications and Network Security (CNS)*, Las Vegas, USA, October 9-11, 2017.

PROGRAMING SKILLS AND LANGUAGES

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