Tianhang Zheng

+16476716884 • th.zheng@mail.utoronto.ca

Google Scholar (Over 650 citations): https://scholar.google.com/citations?user=DDP03z4AAAAJ&hl=en
Github: https://github.com/tianzheng4

Education

- **University of Toronto (UofT)** **Ph.D.** — **Toronto, ON, Canada**
  Electrical and Computer Engineering *GPA: 4.0/4.0* — *2019.9-present*
- **State University of New York at Buffalo (UB)** **M.Sc.** — **Buffalo, NY, U.S.A.**
  Computer Science and Engineering *GPA: 3.89/4.0* — *2017.1 - 2019.6*
- **Peking University (PKU)** **B.Eng.** — **Beijing, China**
  Engineering Structure Analysis (Mechanics) — *2012.9 - 2016.6*

Selected Competitions and Awards

- Distributionally Adversarial Attack (AAAI'19, Oral): rank #1 white-box adversarial attack on MadryLab MNIST Adversarial Examples Challenge in 2018 and rank #3 in 2022.
- NeurIPS'21 Outstanding Reviewer Award 2021
- University of Toronto Fellowship, Department of ECE, University of Toronto 2019
- Best MS Research Award, University at Buffalo 2019
- Award for Academic Excellence, Peking University 2015
- First Award in National Undergraduate Physics Competition 2013

Selected Publications

- **Tianhang Zheng**, Baochun Li "InfoCensor: An Information-Theoretic Framework against Sensitive Attribute Inference and Demographic Disparity" In ACM ASIA Conference on Computer and Communications Security (AsiaCCS'22, Acceptance Rate: 18.4%).
  Note: A framework against attribute inference and group unfairness with information theoretic bounds.
- **Tianhang Zheng**, Baochun Li "Poisoning Attacks on Deep Learning based Wireless Traffic Prediction" In IEEE INFOCOM 2022-IEEE Conference on Computer Communication (INFOCOM'22, Acceptance Rate: 19.9%)
  Note: The first systematic poisoning vulnerability analysis on wireless traffic prediction.
- Hengtong Zhang, **Tianhang Zheng**, Jing Gao, Yaliang Li, Lu Su, Bo Li "Profanity-Avoiding Training Framework for Seq2seq Models with Certified Robustness" In Empirical Methods in Natural Language Processing, 2021 (EMNLP'21, Acceptance Rate: 25.6%)
  Note: A certified framework for training seq2seq models against profanity.
- Yi Zhu, Chenglin Miao, **Tianhang Zheng**, Foad Hajiaghajani, Lu Su, Chunming Qiao "Can We Use Arbitrary Objects to Attack LiDAR Perception in Autonomous Driving?" In ACM Conference on Computer and Communications Security, 2021 (CCS'21, Acceptance Rate: 23.2%)
  Note: A physical adversarial attack against autonomous driving.
- **Tianhang Zheng**, Baochun Li "First-Order Efficient General-Purpose Clean-Label Data Poisoning" In IEEE INFOCOM 2021-IEEE Conference on Computer Communication (INFOCOM'21, Acceptance Rate: 19.9%)
  Note: The earliest first-order general-purpose clean-label data poisoning attack.
- Zhongjie Ba*, **Tianhang Zheng*** (Co-First Author), Xinyu Zhang, Zhan Qin, Baochun Li, Xue Liu, Kui Ren "Learning-based Practical Smartphone Eavesdropping with Built-in Accelerometer" In Proceedings of the 26th Annual Network and Distributed System Security Symposium (NDSS'20, Acceptance Rate: 17.4%) (*equal contribution)
  Note: A practical eavesdropping (privacy) attack on smartphones.
- **Tianhang Zheng**, Changyou Chen, Junsonag Yuan, Bo Li, Kui Ren "PointCloud Saliency Maps" In Proceedings

of the IEEE International Conference on Computer Vision, pp. 1598-1606. 2019 (ICCV'19, **Oral Presentation**, Acceptance Rate: 4.3%)
Note: The first model interpretation method on pointcloud recognition.

- **Tianhang Zheng**, Changyou Chen, Kui Ren "Distributionally adversarial attack" In Proceedings of the AAAI Conference on Artificial Intelligence, vol. 33, pp. 2253-2260. 2019 (AAAI'19, **Oral Presentation**, Acceptance Rate: 16.2%)
Note: The first adversarial attack by distributional optimization.

Selected Github Projects

- Plato: A New Framework for Scalable Federated Learning Research (178 stars, Contributor)
URL: `https://github.com/TL-System/plato`
- PointCloud Saliency Maps (ICCV'19) (68 stars, Individual Contributor)
URL: `https://github.com/tianzheng4/PointCloud-Saliency-Maps`
- Distributionally Adversarial Attack (AAAI'19) (51 stars, Individual Contributor)
URL: `https://github.com/tianzheng4/Distributionally-Adversarial-Attack`
- Learning Speech from Accelerometer Measurements (NDSS'20) (Individual Contributor)
URL: `https://github.com/tianzheng4/learning_speech_from_accelerometer`
- Poisoning Attacks on Wireless Traffic Prediction (INFOCOM'22) (Individual Contributor)
URL: `https://github.com/iQua/poisoning-attacks-wireless-traffic-prediction`
- InfoCensor (AsiaCCS'22) (Individual Contributor)
URL: `https://github.com/iQua/InfoCensor`

Full Publication List

Conference Proceedings

1. **Tianhang Zheng**, Baochun Li "InfoCensor: An Information-Theoretic Framework against Sensitive Attribute Inference and Demographic Disparity" In ACM ASIA Conference on Computer and Communications Security (AsiaCCS'22, Acceptance Rate: 18.4%).
2. **Tianhang Zheng**, Baochun Li "Poisoning Attacks on Deep Learning based Wireless Traffic Prediction" In IEEE INFOCOM 2022-IEEE Conference on Computer Communication (INFOCOM'22, Acceptance Rate: 19.9%)
3. Yi Zhu, Chenglin Miao, **Tianhang Zheng**, Foad Hajiaghajani, Lu Su, Chunming Qiao "Can We Use Arbitrary Objects to Attack LiDAR Perception in Autonomous Driving?" In ACM Conference on Computer and Communications Security, 2021 (CCS'21, Acceptance Rate: 23.2%)
4. Hengtong Zhang, **Tianhang Zheng**, Jing Gao, Yaliang Li, Lu Su, Bo Li "Profanity-Avoiding Training Framework for Seq2seq Models with Certified Robustness" In Empirical Methods in Natural Language Processing, 2021 (EMNLP'21, Acceptance Rate: 25.6%)
5. **Tianhang Zheng**, Baochun Li "First-Order Efficient General-Purpose Clean-Label Data Poisoning" In IEEE INFOCOM 2021-IEEE Conference on Computer Communication (INFOCOM'21, Acceptance Rate: 19.9%)
6. Zhongjie Ba*, **Tianhang Zheng***, Xinyu Zhang, Zhan Qin, Baochun Li, Xue Liu, Kui Ren "Learning-based Practical Smartphone Eavesdropping with Built-in Accelerometer" In Proceedings of the 26th Annual Network and Distributed System Security Symposium (NDSS'20, Acceptance Rate: 17.4%) (*equal contribution)
7. **Tianhang Zheng**, Changyou Chen, Junsong Yuan, Bo Li, Kui Ren "PointCloud Saliency Maps" In Proceedings of the IEEE International Conference on Computer Vision, pp. 1598-1606. 2019 (ICCV'19, Oral Presentation, Acceptance Rate: 4.3%)
8. **Tianhang Zheng**, Changyou Chen, Kui Ren "Distributionally adversarial attack" In Proceedings of the AAAI Conference on Artificial Intelligence, vol. 33, pp. 2253-2260. 2019 (AAAI'19, Oral Presentation, Acceptance Rate: 16.2%)
9. Hengtong Zhang, **Tianhang Zheng**, Jing Gao, Chenglin Miao, Lu Su, Yaliang Li, Kui Ren "Data poisoning attack against knowledge graph embedding" In Proceedings of the 28th International Joint Conference on Artificial Intelligence, AAAI Press, 2019 (IJCAI'19, Acceptance Rate: 17.9%)
10. Qi Wei, Kai Fan, Wenlin Wang, **Tianhang Zheng**, Chakraborty Amit, Katherine Heller, Changyou Chen, Kui Ren "InverseNet: Solving Inverse Problems of Multimedia Data with Splitting Networks" In 2019 IEEE International Conference on Multimedia and Expo, pp. 1324-1329. IEEE, 2019 (ICME'19, Acceptance Rate: 30%)

11. **Tianhang Zheng**, Zhi Sun, Kui Ren "FID: Function Modeling-based Data-Independent and Channel-Robust Physical-Layer Identification" In IEEE INFOCOM 2019-IEEE Conference on Computer Communications (INFOCOM'19, Acceptance Rate: 19.7%)

Journals

1. Mengdi Huai, **Tianhang Zheng**, Chenglin Miao, Liuyi Yao, Aidong Zhang "On the Robustness of Metric Learning: An Adversarial Perspective" In ACM Transactions on Knowledge Discovery from Data (TKDD).
2. Mengnan Zhao, Bo Wang, Wei Wang, Yuqiu Kong, **Tianhang Zheng**, Kui Ren "Guided Erasable Adversarial Attack (GEAA) towards Shared Data Protection" In IEEE Transactions on Information Forensics & Security (TIFS).
3. Kui Ren, **Tianhang Zheng**, Zhan Qin, and Xue Liu. "Adversarial Attacks and Defenses in Deep Learning" In Engineering (2020).

Preprints

1. **Tianhang Zheng***, Di Wang*, Baochun Li, and Jinhui Xu. "Towards Assessment of Randomized Mechanisms for Certifying Adversarial Robustness." arXiv preprint arXiv:2005.07347 (2020) (*equal contribution).
2. **Tianhang Zheng**, Sheng Liu, Changyou Chen, Junsong Yuan, Baochun Li, and Kui Ren. "Towards Understanding the Adversarial Vulnerability of Skeleton-based Action Recognition." arXiv preprint arXiv:2005.07151 (2020).

Academic History at University of Toronto

- ECE1784H Trustworthy Machine Learning (A+)
- ECE1502H Information Theory (A)
- ECE1771H Quality of Service (A+)
- ECE1504H Statistical Learning (A+)
- ECE1505H Convex Optimization (A+)

Teaching Experience

- Teaching Assistant in ECE1505 (UofT): Convex Optimization 2021
- Teaching Assistant in ESC180 (UofT): Introduction to Computer Programming 2020
- Teaching Assistant in CSE191 (UB): Discrete Structures 2018
- Teaching Assistant in CSE574 (UB): Introduction to Machine Learning 2017
- Teaching Assistant in CSE111 (UB): Great Ideas in Computer Science 2017

Professional Activities

Program Committee Member

- **AAAI:** AAAI Conference on Artificial Intelligence 2021, 2022

Reviewer for Conferences

- **NeurIPS:** Neural Information Processing Systems 2021, 2022
- **ICML:** International Conference on Machine Learning 2022
- **ICCV:** International Conference on Computer Vision 2021
- **CVPR:** IEEE Conference on Computer Vision and Pattern Recognition 2021

Reviewer for Journals

- IEEE Transactions on Dependable and Secure Computing
- IEEE Transactions on Pattern Analysis and Machine Intelligence

Professional Skills

- **Programming:** Python (tensorflow & pytorch), C++, CUDA
- **Language Proficiency:** English (proficient), Chinese (native)
- **Other Skills**: Strong background in Mathematics, Physics, Machine Learning, Computer Vision, Computer Security, and Differential Privacy.