Tianhang Zheng

tzheng@umkc.edu

Google Scholar: https://scholar.google.com/citations?user=DDP03z4AAAAJ&hl=en

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*

Competitions and Awards

- Distributionally Adversarial Attack: rank #1 white-box adversarial attack on MadryLab MNIST Adversarial Examples Challenge in 2018 and rank #3 in 2022.
- NeurIPS 2021 Outstanding Reviewer Award 2021
- Best MS Research Award, Department of Computer Science and Engineering, University at Buffalo 2019

Publications

Conference Proceedings

1. **Tianhang Zheng**, Baochun Li. "RDM-DC: Poisoning Resilient Dataset Condensation with Robust Distribution Matching." Uncertainty in Artificial Intelligence. PMLR, 2023 (UAI'23).
2. **Tianhang Zheng**, Hao Lan, and Baochun Li."Be Careful with PyPI Packages: You May Unconsciously Spread Backdoor Model Weights." Proceedings of Machine Learning and Systems 5 (MLSys'23).
3. **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).
4. **Tianhang Zheng**, Baochun Li "Poisoning Attacks on Deep Learning based Wireless Traffic Prediction" In IEEE INFOCOM 2022-IEEE Conference on Computer Communication (INFOCOM'22)
5. 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)
6. 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)
7. **Tianhang Zheng**, Baochun Li "First-Order Efficient General-Purpose Clean-Label Data Poisoning" In IEEE INFOCOM 2021-IEEE Conference on Computer Communication (INFOCOM'21)
8. 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) (*equal contribution)
9. **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**)

10. **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**)
11. 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)
12. 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)
13. **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)

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).

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