Zhi Chen

zhic4@illinois.edu ⬨ (+1) 510-345-7211

Work Experience:

Research Assistant, University of Illinois at Urbana-Champaign ***Jan 2021-Present***

- Conducted selective backdoor attack to subvert malware classifiers.
- Analyzed feature-space concept drift in malware detectors.

Teaching Assistant, University of Illinois at Urbana-Champaign ***Aug 2021-Present***

- CS 463: Computer Security II (Spring 2023)
- CS 445: Computational Photography (Fall 2020)

Research Assistant, University of California, Berkeley ***May 2018-Aug 2020***

- Conducted lifelong anomaly detection through unlearning.
- Implemented a practical method called NDSGD to improve robustness of deep learning model on noisy dataset.
- Implemented robust enhancement for community detection in complex networks.
- Implemented time-aware gradient attack on dynamic network link prediction.
- Implemented domain adaptation for road-object segmentation.
- Conducted autonomous driving with SqueeezeNet and CNN.

Education:

University of Illinois at Urbana-Champaign ***Aug 2020-Present***

- Degree & Major: Ph.D. in Computer Science
- Related coursework: Advanced courses on Computer Science, Machine Learning for Systems, Networks, and Security, Thesis Research
- Research project: Analysis of feature-space concept drift in malware detectors

University of California, Berkeley ***Aug 2019-May 2020***

- Degree & Major: M.S. in Electrical Engineering and Computer Sciences
- Related coursework: Graduate-level courses on Neural Networks and Optimization Models, Individual Research
- Research project: Development of NDSGD method to improve robustness of deep learning model on noisy Dataset

University of California, Berkeley ***Aug 2016-May 2019***

- Degree & Major: B.S. Honors in Electrical Engineering and Computer Sciences
- Related coursework: Courses on Computer Science, Machine Structures, Signals and Systems, Data Structures, and Artificial Intelligence
- Research project: Autonomous driving with SqueezeNet and CNN
- Honors & Awards: B.S. Honors (May 2019), Dean’s List (Spring 2017 & Spring 2018)

Publications:

• Limin Yang, **Zhi Chen**, Jacopo Cortellazzi, Feargus Pendlebury, Kevin Tu, Fabio Pierazzi, Lorenzo Cavallaro, Gang Wang. **Jigsaw Puzzle: Selective Backdoor Attack to Subvert Malware Classifiers**. Proceedings of *The 44th IEEE Symposium on Security and Privacy (S&P),* San Francisco, CA, May 2023.
Summary: We focus on Android malware classifiers and investigate backdoor attacks under the clean-label setting.

• **Zhi Chen**, Zhenning Zhang, Zeliang Kan, Limin Yang, Jacopo Cortellazzi, Feargus Pendlebury, Fabio Pierazzi, Lorenzo Cavallaro, Gang Wang. **Is It Overkill? Analyzing Feature-Space Concept Drift in Malware Detectors.** Proceedings of *The 6th Deep Learning Security and Privacy Workshop (DLSP)*, in conjunction with *The 44th IEEE Symposium on Security and Privacy (IEEE SP*), San Francisco, CA, May 2023.
Summary: We design experiments to empirically analyze the impact of feature-space drift and compare it with data-space drift.

• Jinyin Chen, Jian Zhang, **Zhi Chen**, Min Du, Qi Xuan. **Time-aware Gradient Attack on Dynamic Network Link Prediction.** Proceedings of *The IEEE Transactions on Knowledge and Data Engineering (TKDE)*, February 2023.
Summary: We present the first study of adversarial attack on dynamic network link prediction (DNLP).

• Jiajun Zhou*, Zhi Chen*, Min Du, Lihong Chen, Shanqing Yu, Guanrong Chen, Qi Xuan. **RobustECD: Enhancement of Network Structure for Robust Community Detection.** Proceedings *of The IEEE Transactions on Knowledge and Data Engineering (TKDE)*, January 2023. (* indicates equal contribution)
Summary: We explore robust community detection by enhancing network structure, with two generic algorithms presented.

• **Zhi Chen. NDSGD: A Practical Method to Improve Robustness of Deep Learning Model on Noisy Dataset.** *Technical Report No. UCB/EECS-2020-55*, EECS Department, University of California, Berkeley, May 2020.
Summary: We propose a novel approach called Noisy Dataset Stochastic Gradient Descent (NDSGD) to optimize each step of stochastic gradient descent to improve the robustness of deep learning models.

• Min Du, **Zhi Chen**, Chang Liu, Rajvardhan Oak, Dawn Song**. Lifelong Anomaly Detection Through Unlearning.** Proceedings of *The 26th ACM Conference on Computer and Communications Security (CCS)*, London, UK, November 2019.
Summary: We explore the lifelong anomaly detection problem and propose novel approaches to handle corresponding challenges.