Zhi Chen

387 Soda Hall, Berkeley, CA 94720
zhichen98@berkeley.edu ◇ (+1) 510-345-7211 ◇ https://www.linkedin.com/in/zhichen98

EDUCATION

University of California, Berkeley *Aug 2019 - May 2020 (expected)*
M.S. in Electrical Engineering and Computer Sciences, GPA: 4.00/4.00
Advisor: Professor Dawn Song

University of California, Berkeley *Aug 2016 - May 2019*
B.S. Honors in Electrical Engineering and Computer Sciences, GPA: 3.77/4.00

Duke University *Jul 2015-Aug 2015*
Summer Session Student, Economics: Game Theory, GPA: 4.00/4.00

PUBLICATIONS/PREPRINTS

- 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 2019)**, pages 1283-1297, London, UK, November 2019 (https://dl.acm.org/citation.cfm?doid=3319535.3363226).
- Jiajun Zhou*, **Zhi Chen***(equal contribution), Min Du, Lihong Chen, Shanqing Yu, Feifei Li, Guanrong Chen, Qi Xuan. **Adversarial enhancement for community detection in networks**. *arXiv*:1911.01670, 2019 (submitted to *IEEE Transactions on Knowledge and Data Engineering*) (https://arxiv.org/abs/1911.01670).
- Jinyin Chen, Jian Zhang, **Zhi Chen**, Min Du, Qi Xuan. **Time-aware gradient attack on dynamic network link prediction**. *arXiv*:1911.10561, 2019 (https://arxiv.org/abs/1911.10561).

RESEARCH EXPERIENCE

Graduate Researcher, Center for Long-Term Cybersecurity, UC Berkeley *Jan 2019-Present*

(Began as an undergraduate research assistant) Supervised by **Professor Dawn Song** and collaborated with postdoctoral researcher Min Du on research projects related to deep learning and security.

- **Lifelong anomaly detection through unlearning**. An implementation of a deep-learning based framework named unlearning for anomaly detection. (1) Developed Long Short-Term Memory (LSTM) models to analyze system log files. (2) Maintained a small memory set of labeled data to prevent catastrophic forgetting. (3) Developed a simple and fast process that avoids the necessity to retrain the system from scratch. (4) Evaluated the proposed approach on three real anomaly detection datasets, the proposed method significantly reduced the numbers of false positives and false negatives (e.g., for Hadoop File System (HDFS) log, a reduction of up to 77.3% for false positives and up to 76.6% for false negatives, under the different thresholds). (**Paper presented in CCS 2019**)
- **NDSGD: A practical method to improve robustness of deep learning model on noisy dataset**. An implementation of a meta approach named Noisy Dataset Stochastic Gradient Descent (NDSGD). NDSGD optimizes each step of stochastic gradient descent to improve the robustness of deep learning models. (1) Applied noisy data clipping and grouping to diminish the influence of noisy data. (2) Incorporated robustness factors to reduce oscillation of the loss curve and tuned hyper-parameters to search for optimal models. (3) Evaluated on the celebrated datasets (i.e., MNIST, NEWS). The experimental results indicate that NDSGD performs better than the standard 9-layer CNN model from Google on noise dataset (In MNIST, surpass 1.64% with 20% noise, surpass 4.17% with 50% noise). (**M.S. Individual Research Project**)
- **Adversarial enhancement for community detection in networks**. Implementations of two adversarial enhancement approaches, named adversarial enhancement via genetic algorithm (AE-GA) and vertex similarity (AE-VS), to improve the performance of existing community detection algorithms. (1) Designed a multi-objective fitness function and an auto-threshold to solve the resolution limit problem and achieve consensus partition. (2) Evaluated in conjunction with six existing community detection algorithms on four real-world networks, the proposed methods achieved a significant improvement in the detection rate with an average relative improvement rate between 10%-30%. (3) Adversarial experiments showed that the proposed methods can rebuild the network structure that was previously destroyed by the adversarial attack, and achieve more robust defense against community detection deception methods. (**Paper presented in *arXiv* & submitted to IEEE TKDE 2019**)

- **Time-aware gradient attack on dynamic network link prediction**. An implementation of an attack method on the Dynamic Network Link Prediction (DNLP). The method, named Time-aware Gradient Attack (TGA), can make Deep Dynamic Network Embedding (DDNE) fail to predict target links. (1) Leveraged the gradient information generated by DDNE across different snapshots to rewire network linkages. The rewiring process takes into account the dynamic natures of real-world systems. (2) Implemented TGA in two ways: one is based on traversal search, named TGA-Tra; the other is simplified with greedy search for efficiency, named TGA-Gre. (3) Evaluated on data from real-world scenarios, TGA improved attack success rate by a margin of 20%-40% on DNLP algorithms. (**Paper presented in** *arXiv*)

Research Assistant, Berkeley Artificial Intelligence Research Lab, UC Berkeley *May 2018-Nov 2018*

Collaborated with PhD student Xiangyu Yue (Advisor: Professor Kurt Keutzer) on research projects related to deep learning.

- **Domain adaptation for road-object segmentation**: Developed a semantic-based scene method which enables to realize 3D-object segmentation from a point-wise label map, using a domain-adaptation training method to reduce the distribution gap between synthetic data and real data so as to enhance the performance of model.
- **Autonomous driving with SqueezeNet and CNN**: Developed Convolutional Neural Network (CNN) models in TensorFlow to classify images; Conducted image segmentation on KITTI dataset and model training based on SqueezeNet and CNN, aiming to collect data from GTA-V (an action-adventure video game) and further using this dataset to train CNN model for autonomous driving.

INDUSTRIAL EXPERIENCE

Research Intern, Database and Storage Lab, Alibaba DAMO Academy, Hangzhou, China *Dec 2018-Jan 2019*

- Participated in a project on database security, i.e., assisted in parsing unstructured, free-text log entries into structured representation and developing LSTM model for detection of abnormal conditions of database.

ORGANIZATIONS

Vice President of Technology, Berkeley International Business Crew (BIBC) *Feb 2019-Present*

Member, Robotics@Berkeley *Sep 2018-Present*

COURSEWORK

- **Upper division & Graduate level**: CS162 Operating Systems and System Programming★CS169 Software Engineering★CS170 Efficient Algorithms and Intractable Problems★CS188 Artificial Intelligence★CS189 Machine Learning★EECS126 Probability and Random Processes★EECS C106A Robotics★EECS C106B Robotic Manipulation and Interaction★EE120 Signals and Systems★EECS227AT Optimization Models in Engineering★CS 282A Designing, Visualizing and Understanding Deep Neural Networks★CS294-26 Image Manipulation, Vision, and Computational Photography

HONORS & AWARDS

- **B.S. Honors**, UC Berkeley *May 2019*
- **Dean's List**, College of Engineering, UC Berkeley *Spring 2017 & Spring 2018*
- **Finalist**, the 67th Intel International Science and Engineering Fair, Phoenix *May 2016*

TECHNICAL SKILLS

- **General**: C++, Python, Java, SQL, Ruby, Ros
- **Tools and Devices**: Pytorch, TensorFlow, Rails, Cucumber

RESEARCH INTERESTS

- **Deep Learning; AI Security**