Yunzhe Tian

Phone: (+86) 13020087266
Email: tianyunzhe@bjtu.edu.cn
Homepage: https://tianyunzhe.github.io

Research Interests

AI security including adversarial examples, robust reinforcement learning and robust graph neural network.

Education

Beijing Jiaotong University Advisor: Prof. Wenjia Niu
Beijing Key Laboratory of Security and Privacy in Intelligent Transportation
Master in Electronic Information (Artificial Intelligence) Sep 2020 - Jun 2022 (expected)

Beijing Information Science & Technology University Beijing, China
Bachelor in Information System & Information Management *GPA: 4.02* Sep 2016 - Jun 2020

Intern and Research Experience

Beijing Jiaotong University
Research Intern Mar, 2021 - Present

- Develop a Professional Domain Knowledge Graph System used for information mining, including semantic-based retrieval, knowledge-based Q&A, etc.
- Advisor: Prof. Wenjia Niu

Knowledge Engineering Group, Tsinghua University
Research Intern Sep, 2019 - Jun, 2020

- Researching on named entity open relation extraction algorithm for Beijing Travel Knowledge Graph.
- Advisor: Prof. Juanzi Li

Knowledge Engineering Group, Tsinghua University
Research Intern Sep, 2018 - Jun, 2019

- Based on the data of Aminer System, making prediction on the research lifespan of scholars via machine learning and deep learning
- Advisor: Dr. Peng Zhang

Publications

Yunzhe Tian, Yike Li, Yingxiao Xiang, Wenjia Niu, Endong Tong, and Jiqiang Liu. Curricular Reinforcement Learning for Robust Policy in Unmanned CarRacing Game. In *NDSS 2021, Workshop on Automotive and Autonomous Vehicle Security (AutoSec).*

Yunzhe Tian, Jiqiang Liu, Endong Tong, Wenjia Niu, Liang Chang, Qi Alfred Chen, Gang Li, and Wei Wang. Towards Revealing Parallel Adversarial Attack on Politician Socialnet of Graph Structure. In *Security and Communication Networks (SCN), 2021.*

Endong Tong, Wenjia Niu, **Yunzhe Tian**, Jiqiang Liu, Thar Baker, Sandeep Verma, and Zheli Liu. A Hierarchical Energy-efficient Service Selection Approach with Qos Constraints for Internet of Things. In *IEEE Transactions on Green Communications and Networking (TGCN), 2021.*

Yalun Wu, Minglu Song, Yike Li, **Yunzhe Tian**, Endong Tong, Wenjia Niu, Bowei Jia, Haixiang Huang, Qiong Li and Jiqiang Liu. Improving Convolutional Neural Network-based Webshell Detection through Reinforcement Learning. In *The 23rd International Conference on Information and Communications Security (ICICS 2021), 2021.*

Tong Chen, Yingxiao Xiang, Yike Li, **Yunzhe Tian**, Endong Tong, Wenjia Niu, Jiqiang Liu, Li Gang and Qi Alfred Chen. Protecting Reward Function of Reinforcement Learning via Minimal and Non-catastrophic Adversarial Trajectory. In *The 40th International Symposium on Reliable Distributed Systems (SRDS 2021), 2021.*

王硕汝, 牛温佳, 童恩栋, 陈彤, 李赫, **田蕴哲**, 刘吉强, 韩臻, 李浥东. 强化学习离线策略评估研究综述. *计算机学报, 2021.*

Yunzhe Tian, Yingdi Wang, Endong Tong, Wenjia Niu, Liang Chang, Qi Alfred Chen, Gang Li, and Jiqiang Liu. Exploring Data Correlation between Feature Pairs for Generating Constraint-based Adversarial Examples. In*IEEE 26th International Conference on Parallel and Distributed Systems (ICPADS 2020), 2020*.

Xinyu Huang, **Yunzhe Tian**, Yifei He, Endong Tong, Wenjia Niu, Chenyang Li, Jiqiang Liu, and Liang Chang. Exposing Spoofing Attack on Flocking-based Unmanned Aerial Vehicle Cluster: A Threat to Swarm Intelligence. In *Security and Communication Networks (SCN), 2020*.

Bowei Jia, **Yunzhe Tian**, Di Zhao, Xiaojin Wang, Chenyang Li, Wenjia Niu, Endong Tong, and Jiqiang Liu. Bidirectional Rnn-based Few-shot Training for Detecting Multi-stage Attack. In *The 16th International Conference on Information Security and Cryptology (INSCRYPT 2020), 2020*.

Qinghua Wen, **Yunzhe Tian**, Xiaohui Zhang, Ruoyun Hu, Jinsong Wang, Lei Hou, and Juanzi Li. Type-aware Open Information Extraction via Graph Augmentation Model. In *China Conference on Knowledge Graph and Semantic Computing (CCKS 2020), 2020*.

Academic Experience

Oral Presentation in **AutoSec Workshop @ NDSS'21** (remote presentation)

Oral Presentation in **Inscrypt 2020**, Guangzhou, China

Oral Presentation in **ICPADS 2020**, Hong Kong, China (remote presentation)

Selected Awards

Excellent Undergraduate of Beijing City 2020

Excellent Undergraduate Thesis of Beijing City 2020

Excellent Undergraduate of Beijing Information Science & Technology University 2020

Excellent Undergraduate Thesis of Beijing Information Science & Technology University 2020

National Scholarship of China 2019

President Scholarship of Beijing Information Science & Technology University 2019

Technical Strengths

Deep Learning Software Stacks:	Pytorch, Tensorflow
Programming Languages:	Proficient with Python, Java