Yunzhe Tian

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

Research Interests

- **AI security** including adversarial attack, robust reinforcement learning and robust graph learning.
- **Explainable AI** for wireless communication systems.

Education

Beijing Jiaotong University *Sep 2022 - Present*
Ph.D. in Cyberspace Security
Advisor: Prof. Wenjia Niu

Beijing Jiaotong University *Sep 2020 - Jun 2022*
Master in Artificial Intelligence
Advisor: Prof. Wenjia Niu

Tsinghua Univerisity *Sep 2018 - Jun 2020*
Visiting Student in Knowledge Engineering Group
Advisors: Prof. Juanzi Li and Dr. Peng Zhang

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

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.*

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 *The IEEE 26th International Conference on Parallel and Distributed Systems (ICPADS 2020), 2020.*

Yike Li, Wenjia Niu, **Yunzhe Tian**, Tong Chen, Zhiqiang Xie, Yalun Wu, Yingxiao Xiang, Endong Tong, Thar Baker, and Jiqiang Liu. Multiagent Reinforcement Learning-Based Signal Planning for Resisting Congestion Attack in Green Transportation. In *IEEE Transactions on Green Communications and Networking (TGCN), 2022.*

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.*

Yingdi Wang, **Yunzhe Tian**, Jiqiang Liu, Wenjia Niu, and Endong Tong. A Training-Based Identification Approach to VIN Adversarial Examples in Path Planning. In *Journal of Circuits, Systems and Computers*, 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.*

Tong Chen, Jiqiang Liu, Yalun Wu, **Yunzhe Tian**, Endong Tong, Wenjia Niu, Yike Li, Yingxiao Xiang, Wei Wang. Survey on Astroturfing Detection and Analysis from an Information Technology Perspective. In *Security and Communication Networks (SCN), 2021.*

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

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**

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

Oral Presentation in **ICPADS 2020**, Hong Kong, China

Selected Awards

Excellent Graduate of Beijing Jiaotong University	2022
Excellent Master Thesis of Beijing Jiaotong University	2022
First Prize in Vulnerability Mining Contest for Olympic Winter Games Beijing	2022
Second Prize in DEF CON 30 Contest AutoDriving CTF	2022
Second Prize in DEF CON 29 Contest AutoDriving CTF	2021
Excellent Undergraduate of Beijing	2020
Excellent Undergraduate Thesis of Beijing	2020
National Scholarship	2019
President Scholarship of Beijing Information Science & Technology University	2019

Technical Strengths

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