Yunzhe Tian

Phone: (+86) 130-2008-7266
Email: tianyunzhe@bjtu.edu.cn
Homepage: https://tianyunzhe.github.io

Research Interests

- **AI security** including adversarial attack, backdoor attack, and privacy attack on AI systems.
- **Explainable AI** to enhance the transparency and trustworthiness of AI systems.
- **Brain-inspired computing** with a focus on applications of spiking neural networks in AI systems.

Education

Beijing Jiaotong University *Sep 2022 - Present*
Beijing Key Laboratory of Security and Privacy in Intelligent Transportation
Ph.D. in Cyberspace Science and Technology Advisor: Prof. Wenjia Niu

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

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

Visiting Experience

Deakin University *Nov 2024 - Mar 2025*
Team for Universal Learning and Intellgient Processing (TULIP)
Visiting Ph.D. Advisor: Prof. Gang Li

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

Publications

First Author

Yunzhe Tian, Yike Li, Kang Chen, Zhenguo Zhang, Endong Tong, Jiqiang Liu, Fangyun Qin, Zheng Zheng, and Wenjia Niu. Towards Label-Efficient Deep Learning-based Aging-related Bug Prediction with Spiking Convolutional Neural Networks. In *Transactions on Emerging Topics in Computing, 2025.*

Yunzhe Tian, Dongyue Xu, Endong Tong, Rui Sun, Kang Chen, Yike Li, Thar Baker, Wenjia Niu, and Jiqiang Liu. Toward Learning Model-Agnostic Explanations for Deep Learning-Based Signal Modulation Classifiers. In *IEEE Transactions on Reliability, 2024.*

Yunzhe Tian, Yike Li, Kang Chen, Endong Tong, Wenjia Niu, Jiqiang Liu, Fangyun Qin, Zheng Zheng. Mitigating Overfitting for Deep Learning-based Aging-related Bug Prediction via Brain-inspired Regularization in Spiking Neural Networks. In *IEEE 34th International Symposium on Software Reliability Engineering Workshops (ISSREW 2023), 2023.*

Yike Li, **Yunzhe Tian (co-first author)**, Endong Tong, Wenjia Niu, and Jiqiang Liu. Robust Reinforcement Learning via Progressive Task Sequence. In *Proceedings of the 32nd International Joint Conference on Artificial Intelligence (IJCAI 2023), 2023.*

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.*

Co-Author

徐冬月, **田蕴哲**, 陈康, 李轶珂, 吴亚伦, 童恩栋, 牛温佳, 刘吉强, 史忠植. 面向信号调制识别的对抗攻击与防御综述. *计算机研究与发展, 2024.*

Jiayin Song, Yike Li, **Yunzhe Tian**, Xingyu Wu, Qiong Li, Endong Tong, Wenjia Niu, Zhenguo Zhang, and Jiqiang Li. Knowledge-Driven Backdoor Removal in Deep Neural Networks via

Reinforcement Learning. In *The 17th International Conference on Knowledge Science, Engineering and Management (KSEM 2024), 2024.*

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.*

Yike Li, **Yunzhe Tian**, Endong Tong, Wenjia Niu, Yingxiao Xiang, Tong Chen, Yalun Wu, and Jiqiang Liu.Curricular Robust Reinforcement Learning via GAN-based Perturbation through Continuously-scheduled Task Sequence. In *TSINGHUA Science and Technology (TST), 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.*

Project Experience

Research on Interpretability of Signal Recognition Based on Residual Attention Networks
Project PI *Apr. 2023 - Dec. 2024*
The Fundamental Research Funds for the Central Universities of China (Grant No. 2023YJS031). (Awarded **Excellent Completion**).

- Proposed a novel model-agnostic explainer for the predictions of black-box signal classifier.
- Developed the first generic quantitative explanation evaluation framework for signal classification.
- **Research Outcome**: A journal paper published in *IEEE Transactions on Reliability, 2024.*

Academic Experience

Oral Presentation in **AUTODRIVING TECH TALK @ BCTF 2022**

Oral Presentation in **AutoSec Workshop @ NDSS'21**

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

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

Selected Awards

Fourth Place in IEEE Trojan Removal Competition (IEEE TRC'22).	2023
Excellent Team in DataCon Big Data Security Analysis Competition	2023
First Prize in Vulnerability Mining Contest for Olympic Winter Games Beijing	2022
Second Prize in DEF CON 30 Contest AutoDriving CTF	2022
Excellent Master Thesis of Beijing Jiaotong University	2022
Second Prize in 第二届全国分布式靶场安全技能大赛	2021
Second Prize in DEF CON 29 Contest AutoDriving CTF	2021
Excellent Undergraduate Thesis of Beijing City	2020
National Scholarship	2019
President Scholarship of Beijing Information Science & Technology University	2019