Yunzhe Tian

Beijing, China · tianyunzhe@bjtu.edu.cn · (+86) 13020087266

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 Third International Workshop on Automotive and Autonomous Vehicle Security (AutoSec) 2021 (part of NDSS), 2021

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. Security and Communication Networks, 2021, 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. IEEE Transactions on Green Communications and Networking, 5(2):645-657, 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. Security and Communication Networks, 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, pages 119-131. Springer, 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 Information Security and Cryptology: 16th International Conference, Inscrypt 2020, Guangzhou, China, December 11-14, 2020, Revised Selected Papers, pages 37-52. Springer International Publishing, 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 2020 IEEE 26th International Conference on Parallel and Distributed Systems (ICPADS), pages 430-437. IEEE, 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