Yike Li

Email: yikeli@bjtu.edu.cn
Homepage: https://li-yike.github.io

Research Interests

AI security including (1) robustness and privacy-preservation in Reinforcement Learning; (2) adversarial attack and defense in Intelligent Signal System.

Education

Beijing Jiaotong University *Sep 2021 - Present*
Beijing Key Laboratory of Security and Privacy in Intelligent Transportation
Ph.D. in Cyberspace Security Advisor: Prof. Wenjia Niu

Beijing Jiaotong University *Sep 2019 - Jun 2021*
Beijing Key Laboratory of Security and Privacy in Intelligent Transportation
Master in Cyberspace Security Advisor: Prof. Wenjia Niu

Hefei University of Technology *Sep 2014 - Jun 2018*
Bachelor in Information Security

Publications

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.*

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), 2022.*

Yike Li, Yingxiao Xiang, Endong Tong, Wenjia Niu, Bowei Jia, Long Li, Jiqiang Liu, and Zhen Han. An Empirical Study on GAN-Based Traffic Congestion Attack Analysis: A Visualized Method. In *Wireless Communications and Mobile Computing (WCMC), 2020.*

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).*

相迎宵, **李轶珂**, 刘吉强, 王潇瑾, 陈彤, 童恩栋, 牛温佳, 韩臻. 面向降频污染攻击的智能交通拥堵态势量化分析. *软件学报, 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.*

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.*

Zhiqiang Xie, Yingxiao Xiang, **Yike Li**, Shuang Zhao, Endong Tong, Wenjia Niu, Jiqiang Liu, and Jian Wang. Security Analysis of Poisoning Attacks Against Multi-agent Reinforcement Learning. In *the 21st International Conference on Algorithms and Architectures for Parallel Processing (ICA3PP 2021), 2021.*

Xu Gao, Jiqiang Liu, **Yike Li**, Xiaojin Wang, Yingxiao Xiang, Endong Tong, Wenjia Niu, and Zhen Han. Queue Length Estimation Based Defence Against Data Poisoning Attack for Traffic Signal Control. In *the 10th International Conference on Intelligent Information Processing (IIP 2020), 2020.*

Academic Experience

Oral Presentation in **CTCIS 2021**, Baoding, China (remote presentation)

Selected Awards

The Vulnerability Mining Competition for Olympic Winter Games Beijing 2022
First Prize 2022

The 17th China Post-Graduate Mathematical Contest in Modeling (Huawei Cup)
Second Prize 2020