Yike Li

Email: yileak823@gmail.com
Homepage: https://li-yike.github.io

RESEARCH INTERESTS

My research interests lie in (1) **AI Security**, with emphasis on robustness and privacy in reinforcement learning, (2) **Intelligent Transportation Security**, focusing on data spoofing attack and defense in intelligent signal system. More recently, I have been focusing on **Scalable Threats** in large-scale reinforcement learning systems.

EDUCATION

Beijing Jiaotong University *Sep. 2021 - Jul. 2025*
Beijing Key Laboratory of Security and Privacy in Intelligent Transportation
Ph.D. in Cyberspace Science and Technology Advisor: Prof. Wenjia Niu

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

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

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

PUBLICATIONS

First Author

[IJCAI'23] **Yike Li**, Yunzhe Tian, Endong Tong, Wenjia Niu and Jiqiang Liu. Robust Reinforcement Learning via Progressive Task Sequence. In *the 32nd International Joint Conference on Artificial Intelligence, 2023.* **(CCF-A, Acceptance rate 14.1% = 643/4566)**

[TDSC'23] **Yike Li**, Jiayin Song, Yunzhe Tian, Endong Tong, Yuling Liu, Guozhu Meng, Yalun Wu, Jianhua Li, Wenjia Niu, and Jiqiang Liu. Towards Preventing Imitation Learning Attack via Policy Confusion Defense. (Under Second Review) Summited to *IEEE Transactions on Dependable and Secure Computing, 2023.* **(CCF-A, IF=7.0)**

[TGCN'22] **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, 2022.* **(IF=5.3)**

[TST'22] **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, 2022.* **(IF=5.2)**

[WCMC'20] **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, 2020.*

Co-Author

[TETC'24] Yunzhe Tian, **Yike Li**, Kang Chen, Zhenguo Zhang, Endong Tong, Jiqiang Liu, Fangyun Qin, Zheng Zheng, Wenjia Niu. Towards Label-Efficient Dep Learning-based Aging-rcelated Bug Prediction with Spiking Convolutional Neural Nctworks. (Under Second Review) Submmited to *IEEE Transactions on Emerging Topics in Computing, 2024.*

[KSEM'24] Jiayin Song, **Yike Li**, Yunzhe Tian, Xingyu Wu, Qiong Li, Endong Tong, Wenjia Niu, Zhenguo Zhang, and Jiqiang Liu. Knowledge-Driven Backdoor Removal in Deep Neural Networks via Reinforcement Learning. In *the 17th International Conference on Knowledge Science, Engineering and Management, 2024.*

[TRE'24] Yunzhe Tian, Dongyue Xu, Endong Tong, Rui Sun, Kang Chen, **Yike Li**, Thar Baker, Wenjia Niu, Jiqiang Liu. Toward Learning Model-Agnostic Explanations for Deep Learning-Based Signal Modulation Classifiers. In *IEEE Transactions on Reliability, 2024.*

[WoSAR'23] 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 *the 16th International Workshop on Software Aging and Rejuvenation, 2023.*

[TAI'23] Tong Chen, Jiqiang Liu, Thar Baker, Yalun Wu, Yingxiao Xiang, **Yike Li**, Wenjia Niu, Endong Tong, Albert Y. Zomaya. A Mutual Information-Based Assessment of Reverse Engineering on Rewards of Reinforcement Learning. In *IEEE Transactions on Artificial Intelligence, 2023.*

[ITIS'22] Yingxiao Xiang, Chao Li, Tong Chen, **Yike Li**, Endong Tong, Wenjia Niu, Qiong Li, Jiqiang Liu, Wei Wang. Toward Blockchain-Based Spoofing Defense for Controlled Optimization of Phases in Traffic Signal System. In *IEICE TRANSACTIONS on Information and Systems, 2022.*

[JS'21] Yingxiao Xiang, **Yike Li**, Jiqiang Liu, Xiaojin Wang, Tong Chen, Endong Tong, Wenjia Niu and Zhen Han. Quantified Analysis of Congestion Situation in Intelligent Transportation Towards Frequency-reduced Spoofing Attack. In *Journal of Software, 2023.* (In Chinese)

[AutoSec'21] 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.*

[SRDS'21] 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, 2021.*

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

[ICICS'21] Yalun Wu, Minglu Song, **Yike Li**, Yunzhe Tian, Endong Tong, Wenjia Niu, Bowei Jia, Haixiang Huang, Qiong Li, Jiqiang Liu. Improving Convolutional Neural Network-Based Webshell Detection Through Reinforcement Learning In *the 23rd International Conference on Information and Communications Security, 2021.*

[IIP'20] Xu Gao, Jiqiang Liu, **Yike Li**, Xiaojin Wang, Yingxiao Xiang, Endong Tong, Wenjia Niu, Zhen Han. Queue Length Estimation Based Defence Against Data Poisoning Attack for Traffic Signal Control. In *the 11th International Conference on Intelligent Information Processing, 2020.*

PROJECT EXPERIENCE

Project PI

Research on Reinforcement Learning Robustness Based on Curriculum Task Generation *Apr. 2022 - Mar. 2024*

The Fundamental Research Funds for the Central Universities of China (Grant No. 2022YJS023). (Awarded **Excellent Completion**).

- Proposed the "Max-Expectation" formulation for robust RL compared to "Max-Min" formulation.
- Developed an algorithm via progressive learning to solve the "Max-Expectation" problem.
- **Research Outcome**: A conference paper published in IJCAI 2023.

Project Member

Research on Multi-Agent Collaborative Defense Against Data Poisoning Attacks in Intelligent Traffic Signal Systems *Oct. 2019 - Dec. 2023*

The National Natural Science Foundation of China (Grant No. 61972025).

- Built an Intelligent Traffic Signal System (I-SIG) using MMITSS from the USDOT program, with PTV VISSIM as the simulation software and COP+EVLS as the signal control algorithm.
- Deployed the I-SIG system in a real-world setting on Xinshi Trial Road in Shijiazhuang, China.
- Developed a multi-intersection collaborative signal planning algorithm based on multi-agent RL to defend against data poisoning attacks, improving both traffic efficiency and energy efficiency.
- **Research Outcome**: A journal paper published in TGCN 2022.

Testing of Deep Reinforcement Learning Software Systems: An Approach Driven by Coverage of Markov Decision Sequence Relation *Jan. 2024 - Present*

The National Natural Science Foundation of China (Grant No. 62372021).

- Constructed a dataset of real-world RL-related bugs from *Stack Overflow* and *Github*.
- Studied the root causes and symptoms of these failures, providing valuable insights for RL testing.
- **Research Outcome**: A journal paper under review in TDSC.

TEACHING & MENTORING EXPERIENCE

Teaching Assistant *Jun. 2021 - Jul. 2021*
80S504Q: Information Security Professional Practice and Training I. Instructor: Prof. Wenjia Niu

Teaching Assistant *Feb. 2021 - Apr. 2022*
M602031B: Situation Awareness of Cyberspace Security I. Instructor: Prof. Wenjia Niu

Guest Lecturer *Feb. 2023 - Aug. 2023*
M402055B: Artificial Intelligence Security. Instructor: Prof. Wenjia Niu
Guest Lecture on Reinforcement Learning Security

Research Advising and Mentoring
Team leader for the RL group, a subgroup within the THETA Lab led by Prof. Wenjia Niu.

- Yunzhe Tian (BJTU M.S., now Ph.D. at BJTU) *Sep. 2020 - Jul. 2022*
  Awarded **Outstanding Master Thesis of Beijing Jiaotong University**
- Shiyao Chen (BJTU M.S., now at CMCC) *Sep. 2021 - Jul. 2024*
  Awarded **Outstanding Master Thesis of Beijing Jiaotong University**
- Zhenglong Liu (BJTU B.S., now M.S. at USC) *May. 2022 - Jul. 2024*
  Awarded **National-level College Student Innovative Training Program**

ACADEMIC EXPERIENCE

Reviewer of Journal of Information and Knowledge Management (JIKM).
Reviewer of Journal of Intelligent & Fuzzy Systems (JIFS).
Oral Presentation in CTCIS 2021, Baoding, China.
Oral Presentation in IJCAI 2023, Macao, China.

SELECTED AWARDS

Beijing Jiaotong University First-class Doctoral Academic Scholarship *2022, 2023, 2024*

The 34th Huiguang Cup Academic Cultural Festival
Second Prize, Academic Poster Track *2024*

The DataCon Big Data Security Analysis Competition
Team First Prize, AI security Track *2023*

IEEE Trojan Removal Competition at ICLR 2023.
Fourth Place *2023*

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

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

SKILLS

Programming Languages: Python, C++, Matlab
Deep Learning Software Stacks: PyTorch, Tensorflow, RLlib, Tianshou, Stable-Baselines
Technical & Collaborative Tools: Git, Latex, Visio, Zotero
Natural Languages: Mandarin Chinese (Native), English (Proficient)

ACADEMIC REFERENCES

- Prof. Wenjia Niu
  niuwj@bjtu.edu.cn, (+86)13811762155, Beijing Jiaotong University
- Assoc. Prof. Endong Tong
  edtong@bjtu.edu.cn, (+86)15101049490, Beijing Jiaotong University