Chengze Du

ducz.Monickar@gmail.com| https://Monickar.github.io

EDUCATION

Beijing University of Posts and Telecommunications(BUPT) Beijing, China

Bachelor of Science in Information Security, School of Cyberspace Security *Sep. 2021 – Present*

- Average Scores: 87/100 (GPA: 3.56/4)
- The Second Prize Scholarship **(top 15%)**

REARCH INTERESTS

Network Tomography, Deep Learning, Differential Privacy, Artificial intelligence of things

PUBLICATIONS & PATENTS

[1]Chengze Du, Jibin Shi, Ying Zhang, Renda Han (2025). GuidedLatent: Defending VAEs against Membership Inference Attacks via Distribution-Guided Privacy. *International Joint Conference on Neural Networks (IJCNN 2025).*

[2]Chengze Du, Jibin Shi (2025). SecureNT: A Practical Framework for Efficient Topology Protection and Monitoring. *Under Review at International Conference on Security and Privacy in Communication Networks (Securecomm 2025)*

[3]Chengze Du, Zhiwei Yu, Xiangyu Wang (2024). Identification of Path Congestion Status for Network Performance Tomography using Deep Spatial-Temporal Learning. *Under Revision at Computer Communications.*

[4]Chengze Du, Shengli Pan, Chengbo Jiao. (2024). End-to-End Identification of Network Path Congestion Status Based on Adversarial Autoencoders. *Chinese Patent.*(Substantive Examination)

REARCH EXPERIENCE

Undergraduate Research Assistant@BUPT Beijing, China

***Project 1**:Identifying Path Congestion Status for Network Tomography with Deep Learning* *Nov. 2023 – Present*

- Advisors: Prof. Shengli Pan
- **Description:** This project improves network tomography by introducing the concept of Additive Congestion Status to address limitations in accurately identifying congested network links. By integrating Adversarial Autoencoders (AAE) with Long Short-Term Memory (LSTM) networks, our method categorizes and quantifies congestion, leveraging spatio-temporal data to enhance link performance inference and congestion localization, outperforming traditional threshold-based algorithms.
- **Contributions:** Methodology, experiments, data analysis/visualization, writing
- **Achievements:** Authored and submitted the research paper as the first author, and applied for a patent as the primary inventor.

***Project 2**: Adversarial Network Boolean Tomography* *Jun. 2023 – Apr. 2024*

- Advisors: Prof. Shengli Pan, Prof. Jinqiao Shi
- **Description:** This project enhances network boolean tomography to detect and localize congestion attacks on network links. By employing multi-timeslot observations and optimizing the F-measure to reduce the False Negative Rate (FNR), our approach improves upon traditional methods, offering more accurate and robust monitoring of network congestion in adversarial environments.
- **Contributions:** Experiments, data analysis/visualization, writing-partly
- **Achievements:** Co-authored and submitted the research paper as the first author in IEEE TNSM.

Work Experience

Zhipu AI, AI Department Beijing, China

Engineering Internship *Oct. 2024 – Jan. 2025*

SKILLS

Languages: Python(Pytorch, Keras, Pandas, SciPy, SkLearn, etc.), C/C++, Bash, Latex

Technologies/Frameworks:: NS-3 Network Simulator, Docker, Server Maintenance (Linux)